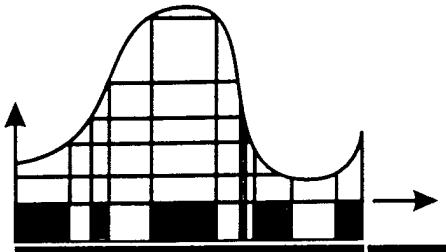

Center for Foundations of Intelligent Systems

Technical Report
98-14

On Hybrid Systems and the Modal μ-calculus

J. M. DAVOREN

November 1998

CORNELL
UNIVERSITY

625 Rhodes Hall, Ithaca, NY 14853 (607) 255-8005

REPORT DOCUMENTATION PAGE

Form Approved
OMB NO. 0704-0188

1. AGENCY USE ONLY (Leave Blank)	2. REPORT DATE 1 March 1999	3. REPORT TYPE AND DATES COVERED TECHNICAL

4. TITLE AND SUBTITLE

ON HYBRID SYSTEMS AND THE MODAL μ-CALCULUS

5. FUNDING NUMBERS

DAAH04-96-1-0341

6. AUTHOR(S)

J.M. DAVOREN

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Regents of the University of California
c/o Sponsored Projects Office
336 Sproul Hall
Berkeley, CA 94720-5940

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

U. S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

ARO 35873.99-MA-MUR

11. SUPPLEMENTARY NOTES

The views, opinions and/or findings contained in this report are those of the author(s) and should not be construed as an official Department of the Army position, policy or decision, unless so designated by other documentation.

12 a. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution unlimited.

12 b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)

Much of the contemporary work in logics for the formal verification of hybrid systems (notably the work of Henzinger at UC Berkeley and Manna at Stanford) builds directly on the framework of temporal logic verification of discrete systems. The core computational model is that of a hybrid automaton, which is represented formally as a *transition system* over a hybrid state space $X \subseteq Q \times I\!R^n$, where Q is a finite set of discrete modes. While the temporal logic framework is adequate to formally express many qualitative dynamic properties of such systems, it fails to capture the "continuity" of continuous dynamics, or to reflect the topological and metric structure of Euclidean space. In addressing this deficiency, we look to the *modal μ-calculus*, a richly expressive formal logic over transition system models, into which virtually all temporal and modal logics can be translated. The key move in this paper is to view the transition system models of hybrid automata not merely as some form of "discrete abstraction", but rather as a skeleton which can be fleshed out by imbuing the state space with *topological, metric tolerance* or other *structure*. Drawing on the resources of modal logics, we give explicit symbolic representation to such structure in polymodal logics extending the modal μ-calculus...

14. SUBJECT TERMS	15. NUMBER OF PAGES
formal verification, hybrid systems, fixed points, modal logic, temporal logic, general topology, continuity, stability	32
	16. PRICE CODE

17. SECURITY CLASSIFICATION OR REPORT	18. SECURITY CLASSIFICATION ON THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

Technical Report
98-14

On Hybrid Systems and the Modal μ-calculus

J. M. DAVOREN

November 1998

On Hybrid Systems and the Modal μ-calculus

J. M. Davoren*

Center for Foundations of Intelligent Systems
626 Rhodes Hall, Cornell University
Ithaca NY 14853, USA
davoren@cornell.edu

Abstract. We start from a basic and fruitful idea in current work on the formal analysis and verification of hybrid and real-time systems: the *uniform* representation of both sorts of state dynamics – both continuous evolution within a control mode, and the effect of discrete jumps between control modes – as *abstract transition relations* over a hybrid space $X \subseteq Q \times \mathbb{R}^n$, where Q is a finite set of control modes. The resulting "machine" or *transition system model* is currently analyzed using the resources of concurrent and reactive systems theory and temporal logic verification, abstracted from their original setting of finite state spaces and purely discrete transitions. One such resource is the *propositional μ-calculus*: a richly expressive formal logic of transition system models (of arbitrary cardinality), which subsumes virtually all temporal and modal logics. The key move here is to view the transition system models of hybrid automata not merely as some form of "discrete abstraction", but rather as a skeleton which can be fleshed out by imbuing the state space with *topological, metric tolerance* or other *structure*. Drawing on the resources of modal logics, we give explicit symbolic representation to such structure in polymodal logics extending the modal μ-calculus. The result is a logical formalism in which we can directly and simply express *continuity properties of transition relations* and metric tolerance properties such as "being within distance ϵ" of a set. Moreover, the logics have sound and complete deductive proof systems, so assumptions of continuity or tolerance can be used as hypotheses in deductive verification. By also viewing transition relations in their equivalent form as *set-valued functions*, and drawing on the resources of set-valued analysis and dynamical systems theory, we open the way to a richer formal analysis of robustness and stability for hybrid automata and related classes of systems.

1 Introduction

It is hardly controversial to claim that the *μ-calculus* is a formal logic of central import for the analysis and verification of hybrid automata and related classes of systems. The fundamental concepts of *reachability* and *invariance* are expressible

* Research supported by the ARO under the MURI program "Integrated Approach to Intelligent Systems", grant no. DAA H04-96-1-0341.

in terms of fixed-points of operators mapping sets of states to sets of states, and are thus definable in the language of the μ-calculus. The iterative computation of the denotation of such fixed point formulas lies at the heart of symbolic model checking tools for hybrid and real-time systems such as HyTech [4], [19] and Kronos [13]. More generally, the propositional μ-calculus is well-recognized as a richly expressive logic over transition system models: the power of its fixed-point quantifiers are such that it subsumes virtually all temporal, modal and dynamic logics [15], [25].

However, the current practice, within the allied field of automated verification of (discrete) reactive systems as well as within the hybrid systems community, is to consider the μ-calculus not as a working or usable logic but rather as a logic of the substratum. It provides a common "machine" language and semantics for verification by model checking, with user-input specifications written in the more "natural" languages of temporal logics, and then translated into that of the μ-calculus.

This paper challenges that practice, and demonstrates that the propositional μ-calculus and various of its modal logic extensions can provide both an expressively rich and "human readable" formalism for reasoning about properties of hybrid dynamical systems.

We begin with the "machine" or transition system models of hybrid systems, in which both sorts of state transformation – continuous evolution within a control mode, and the effects of discrete jumps between control modes – are uniformly represented as *abstract transition relations* $r \subseteq X \times X$ over a hybrid state space $X \subseteq Q \times \mathbb{R}^n$, where Q is a finite set of control modes or discrete states.

Formally, define a *labeled transition system* (LTS) (or *generalized Kripke model*) to be a structure

$$\mathfrak{M} = \left(X, \{a^{\mathfrak{M}}\}_{a \in \Sigma}, \{\|p\|^{\mathfrak{M}}\}_{p \in \Phi}\right) \tag{1}$$

where $X \neq \varnothing$ is the state space (of arbitrary cardinality); for each transition label $a \in \Sigma$, $a^{\mathfrak{M}} \subseteq X \times X$ is a binary relation on X; and for each propositional constant (observation or event label) $p \in \Phi$, $\|p\|^{\mathfrak{M}} \subseteq X$ is a fixed subset of X.

An LTS model is a clean and simple abstraction of a *finite automaton*. Such an $\mathfrak{M}$ is an abstract machine over state space X, with input or action alphabet Σ and transition map $\delta : X \times \Sigma \to \mathcal{P}(X)$ given by: $x' \in \delta(x, a)$ iff $x \xrightarrow{a^{\mathfrak{M}}} x'$. It is additionally equipped with an observation alphabet Φ, and an output map $o : X \to \mathcal{P}(\Phi)$ given by: $o(x) = \{p \in \Phi \mid x \in \|p\|^{\mathfrak{M}}\}$; sets of initial or final states can be identified by specific labels in Φ.

A (basic) hybrid automata $\mathcal{H}$ is typically represented by a graph of the form depicted in Figure 1. Hybrid automata and their associated LTS models are examined in more detail in Section 2; for now, we give a high-level description, based on Henzinger's "time-abstract" transition system in [19] §1.2.

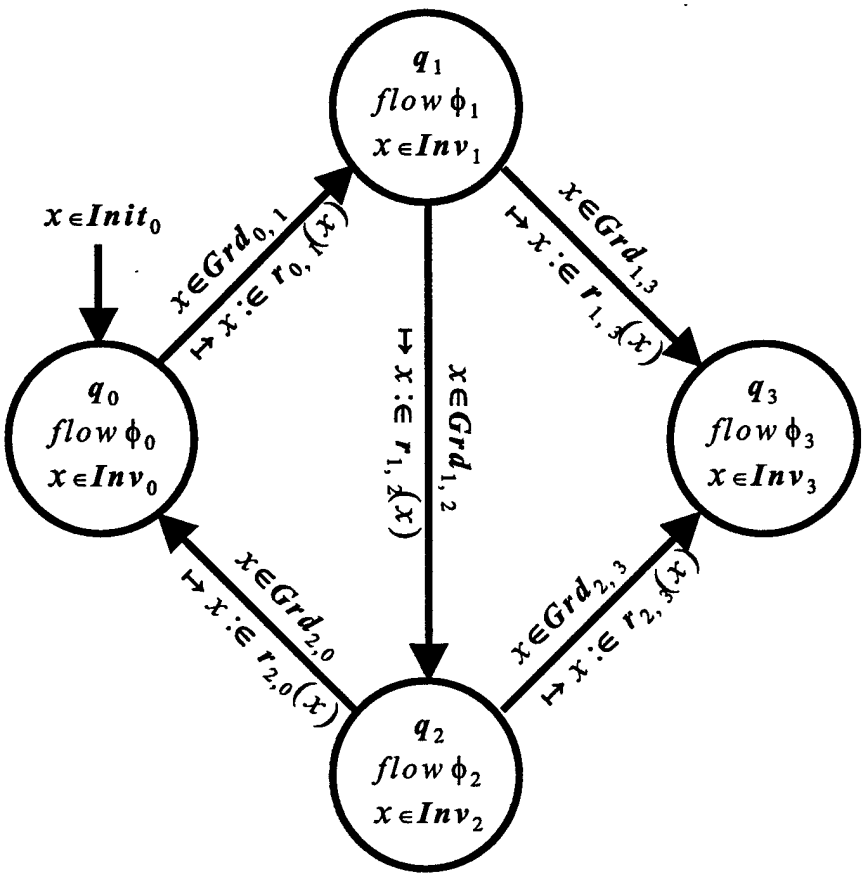

Fig. 1. Basic hybrid automaton

An LTS model $\mathfrak{M}_{\mathcal{H}}$ of a hybrid automaton $\mathcal{H}$ has a state space $X \subseteq Q \times \mathbb{R}^n$, with Q finite. So states are pairs (q, x), where $q \in Q$ and $x = (x_1, ..., x_n) \in \mathbb{R}^n$. For each $q \in Q$, let $X_q \subseteq \mathbb{R}^n$ be the projection of X under q. The transition alphabet Σ will include symbols such as $\mathbf{e}_q$ for the relation of *evolution* (a "time-step" or "continuous transition") within each discrete mode $q \in Q$. In the basic case, such a relation is defined by: $(q, x) \xrightarrow{e_q} (q, x')$ iff there is an integral curve along the flow ϕ_q connecting $x \in X_q$ to $x' \in X_q$, and all points on the curve between x and x' lie inside the invariant set $Inv_q \subseteq X_q$. The transition alphabet will also include, for each edge (q, q') in the discrete transition graph $G \subseteq Q \times Q$ of $\mathcal{H}$, a symbol $\mathbf{c}_{q,q'}$ for the *controlled jump* relation (a "step" or "discrete transition") modeling the effect of making a controlled switch from mode q to mode q'. Such relations are standardly defined by: $(q, x) \xrightarrow{c_{q,q'}} (q', x')$ iff $x \in Grd_{q,q'}$, $x' \in Inv_{q'}$, and $x' \in r_{q,q'}(x)$, where $r_{q,q'} \subseteq X_q \times X_{q'}$ is a reset relation for the real-valued coordinates, and the domain $Grd_{q,q'} \subseteq X_q$ is known

as the guard set of the discrete transition (q, q'). The alphabet Φ of atomic propositions will include $\mathbf{Init}_q$ and $\mathbf{Inv}_q$ for $q \in Q$, and $\mathbf{Grd}_{q,q'}$ for $(q, q') \in G$.

A trajectory of $\mathcal{H}$ is a finite or infinite sequence $\langle \delta_i, q_i, \gamma_i \rangle_{i \in I}$ such that for each $i \in I$: the duration $\delta_i \geq 0$; the curve $\gamma_i : [0, \delta_i] \to X_{q_i}$ is such that $(q_i, \gamma_i(0)) \xrightarrow{e_{q_i}} (q_i, \gamma_i(t))$ for all $t \in [0, \delta_i]$; $(q_i, q_{i+1}) \in G$; and $(q_i, \gamma_i(\delta_i)) \xrightarrow{c_{q_i, q_{i+1}}} (q_{i+1}, \gamma_{i+1}(0))$. When I is finite, with largest element N, it is allowed that $\delta_N = \infty$. When a hybrid automaton is thought of as a discrete controller interacting with a physical plant, the class of trajectories, so defined, are founded on implicit operational assumptions of continuous and perfect precision sensing, and instantaneous control switches ([19]).

In the *modal* – as distinct from *temporal* – variant of the μ-calculus[1], the propositional language (over an alphabet (Σ, Φ)) includes a dual pair of modal operators $[a]$ and $\langle a \rangle$, for each transition label $a \in \Sigma$. The (standard) relational Kripke semantics of the labeled modalities are given by the *universal* and *existential pre-image operators* of the corresponding relations $r = a^{\mathfrak{M}}$. For relations $r \subseteq X \times Y$, and sets $A \subseteq Y$,

$$\begin{aligned} \tau(r)(A) &\triangleq \{\, x \in X \mid (\forall y \in Y)[\, x \xrightarrow{r} y \;\Rightarrow\; y \in A] \,\} \\ \sigma(r)(A) &\triangleq \{\, x \in X \mid (\exists y \in Y)[\, x \xrightarrow{r} y \;\wedge\; y \in A] \,\} \end{aligned} \tag{2}$$

In the notation of [20], $\sigma(r) = \mathrm{pre}[r]$ and $\tau(r) = \widetilde{\mathrm{pre}}[r]$. The semantic readings of the modalities are *forward*-looking, and in temporal logics, they are known as relativized *next* operators:

$$\begin{aligned} [a]\,\varphi &\rightleftharpoons \text{“}\textit{All}\ a\text{-successors satisfy } \varphi\text{”} \\ \langle a \rangle\,\varphi &\rightleftharpoons \text{“}\textit{Some}\ a\text{-successor satisfies } \varphi\text{”} \end{aligned}$$

The temporal variant of the μ-calculus usually works with the *global* transition relation $R^{\mathfrak{M}} = \bigcup_{a \in \Sigma} a^{\mathfrak{M}}$ (standardly assumed to be *total*) and the modal operators are replaced by global temporal "next" operators: $\forall X$ or $\forall \bigcirc$, and $\exists X$ or $\exists \bigcirc$.

Sentences φ of the μ-calculus denote *sets of states* $\|\varphi\|^{\mathfrak{M}} \subseteq X$, and a sentence is *true* in $\mathfrak{M}$, written $\mathfrak{M} \models \varphi$, iff $\|\varphi\|^{\mathfrak{M}} = X$, or equivalently, $\|\neg\varphi\|^{\mathfrak{M}} = \varnothing$. The propositional connectives $\neg$, $\wedge$ and $\vee$ are interpreted by set theoretic complement, intersection and union, and other connectives and constants defined in the usual way. In particular, $\|\mathbf{tt}\|^{\mathfrak{M}} = X$, and an implication $\varphi \to \psi$ is true in $\mathfrak{M}$ exactly when $\|\varphi\|^{\mathfrak{M}} \subseteq \|\psi\|^{\mathfrak{M}}$. As a point of contrast, in the language of *linear temporal logic* **LTL**, sentences denote sets of (finite or infinite) *paths* or *trajectories* of the LTS model, rather than sets of states. In the language of the branching temporal logic **CTL***, there are two sorts of sentences: state sentences, true or false at states of the LTS model, and path sentences, true or

[1] The formal syntax and semantics of the μ-calculus are reviewed in detail in Section 3 below. For an account of the modal and temporal flavors of the μ-calculus, see [38] §4.2. [15] is a good source for translations of various linear and branching time temporal logics into the μ-calculus. For background on modal logics, see [9], [35].

false of infinite paths through the model. An $\exists$ or $\forall$ path quantifier applied to a path sentence produces a state sentence, and such quantification is definable using the least and greatest fixed-point quantifiers of the μ-calculus.

The principal advantage of working in the modal rather than temporal framework is that it gives a *modular* specification language for expressing properties of transition systems: we can describe and reason about each of the *component* transition relations of an LTS model, and how they are combined to form more complex transition relations. In particular, we can give a clean and modular formal description of classes of trajectories of the system.

The modal sentences:

$$\psi \to [\mathbf{c}_{q,q'}]\varphi \quad \text{and} \quad \psi \to [\mathbf{e}_q]\varphi$$

with the semantic readings "If ψ holds, then all $\mathbf{c}_{q,q'}$-successors satisfy φ", and likewise for $\mathbf{e}_q$, correspond precisely to Manna and Pnueli's two types of (temporal logic) safety verification conditions for hybrid systems in [29] §4.1. Their notation is: $\{\psi\}\tau\{\varphi\}$ and $\{\psi\}cont\{\varphi\}$, respectively, where τ ranges over jump transitions and "*cont*" denotes the union of all the evolution relations.

The modal sentence

$$\langle \mathbf{e}_{q_0}\rangle\langle \mathbf{c}_{q_0,q_1}\rangle\langle \mathbf{e}_{q_1}\rangle\langle \mathbf{c}_{q_1,q_2}\rangle\langle \mathbf{e}_{q_2}\rangle \cdots \langle \mathbf{e}_{q_{k-1}}\rangle\langle \mathbf{c}_{q_{k-1},q_k}\rangle\langle \mathbf{e}_{q_k}\rangle\, \varphi \tag{3}$$

denotes the set of states (q_0, x) from which *some* trajectory with discrete trace $(q_0, q_1, \ldots, q_k)$ *reaches* the set $\|\varphi\|^{\mathfrak{M}} \subseteq X$. Dually, the modal sentence

$$[\mathbf{e}_{q_0}][\mathbf{c}_{q_0,q_1}][\mathbf{e}_{q_1}][\mathbf{c}_{q_1,q_2}][\mathbf{e}_{q_2}] \cdots [\mathbf{e}_{q_{k-1}}][\mathbf{c}_{q_{k-1},q_k}][\mathbf{e}_{q_k}]\, \varphi \tag{4}$$

denotes the set of states from which *all* $(q_0, q_1, \ldots, q_k)$-trajectories *reach* the set $\|\varphi\|^{\mathfrak{M}}$, upon the last jump c_{q_{k-1},q_k} and remain in $\|\varphi\|^{\mathfrak{M}}$ throughout the last evolution e_{q_k}.

Defining $\mathbf{e}$ and $\mathbf{c}$ to denote the relational sum (union) of, respectively, the relations for the $\mathbf{e}_q$'s for $q \in Q$, and the relations for the $\mathbf{c}_{q,q'}$'s for $(q, q') \in G$, the dynamics of the class of all hybrid trajectories with finite discrete traces are captured by the dual fixed-point definable modalities:

$$\langle \mathbf{h}\rangle\, \varphi \triangleq \mu Z.\, \langle \mathbf{e}\rangle\varphi \vee \langle \mathbf{e}\rangle\langle \mathbf{c}\rangle Z \quad \text{and} \quad [\mathbf{h}]\, \varphi \triangleq \nu Z.\, [\mathbf{e}]\varphi \wedge [\mathbf{e}][\mathbf{c}]Z \tag{5}$$

The sentence $\langle \mathbf{h}\rangle\, \varphi$ "unwinds" to the infinite union of all sentences of the form (3), and dually, $[\mathbf{h}]\, \varphi$ corresponds to the intersection of all sentences of the form (4). As a regular expression, we have $\mathbf{h} = (\mathbf{ec})^*\mathbf{e} = \mathbf{e}(\mathbf{ce})^*$ (so we are in fact working in the weaker propositional dynamic logic **PDL**, rather than the full μ-calculus.) Semantically, $\langle \mathbf{h}\rangle$ and $[\mathbf{h}]$ correspond to the dual pre-image operators of the *reachability relation* h of the system under the control of $\mathcal{H}$; that is, $(q, x) \xrightarrow{h} (q', x')$ iff some trajectory $\langle \delta_i, q_i, \gamma_i\rangle_{i \in I}$ with $q_0 = q$ and $\gamma_0(0) = x$ passes through the point (q', x').

We now have the formal linguistic machinery to succinctly express various system specifications. The *safety* sentence

$$\mathbf{Init} \to [\mathbf{h}]\, \varphi \tag{6}$$

is *true* in the model $\mathfrak{M} = \mathfrak{M}_{\mathcal{H}}$ exactly when every trajectory that starts in the set $\|\mathbf{Init}\|^{\mathfrak{M}}$ *always* remains within $\|\varphi\|^{\mathfrak{M}}$. More generally, we say a set $\|\varphi\|^{\mathfrak{M}}$ is *future-invariant* under $\mathcal{H}$ exactly when the sentence $\varphi \to [\mathbf{h}]\,\varphi$ is true in $\mathfrak{M}$. We also have at our disposal (previously unutilized) *deductive proof systems* for the μ-calculus, such as Kozen's axiomatization $\mathbf{L}_\mu$ [23], [5], [40], which is sound and complete over *arbitrary* LTS models. From the fixed-point rules of $\mathbf{L}_\mu$ (given in Section 5), one readily derives an obvious *invariance rule* for hybrid trajectories:

$$\frac{\psi \to \varphi \quad \varphi \to [\mathbf{e}_q]\varphi \quad \varphi \to [\mathbf{c}_{q,q'}]\varphi}{\psi \to [\mathbf{h}]\varphi} \quad \text{for } q \in Q,\ (q,q') \in G \tag{7}$$

This is a simpler μ-calculus analog of the **LTL** invariance rule used in the verification of safety properties for hybrid automata in [29], [30].

To express liveness properties, we use modal analogs of the "box-diamond" construct in temporal logic. For example, the sentence

$$\varphi \to [\mathbf{h}]\langle \mathbf{e}\rangle\langle \mathbf{c}\rangle\langle \mathbf{e}\rangle\,\mathbf{tt} \tag{8}$$

is true in $\mathfrak{M}$ exactly when every maximal $\mathcal{H}$ trajectory from a state in $\|\varphi\|^{\mathfrak{M}}$ has an *infinite* discrete trace. This is so because $[\mathbf{h}]\langle \mathbf{e}\rangle\langle \mathbf{c}\rangle\langle \mathbf{e}\rangle\,\mathbf{tt}$ denotes the set of states from which every trajectory with a finite discrete trace can be properly extended. Similarly, the sentence $\varphi \to [\mathbf{h}]\langle \mathbf{e}\rangle\langle \mathbf{c}\rangle\langle \mathbf{e}\rangle\varphi$ is true in $\mathfrak{M}$ exactly when every trajectory from $\|\varphi\|^{\mathfrak{M}}$ returns to $\|\varphi\|^{\mathfrak{M}}$ via a controlled jump *infinitely often*. And $[\mathbf{h}]\langle \mathbf{h}\rangle\varphi$ denotes the set of states from which every hybrid trajectory *eventually* reaches $\|\varphi\|^{\mathfrak{M}}$. Note that at this level of description, we cannot expressly rule out *Zeno* trajectories $\langle \delta_i, q_i, \gamma_i\rangle_{i\in I}$ such that I is infinite but $\sum_{i\in I}\delta_i < \infty$, but by considering variant evolution relations $\hat{e}_q$ defined using a minimal time duration δ, we could.

A clean μ-calculus definition of the higher-order modalities $\langle \mathbf{h}\rangle$ and $[\mathbf{h}]$ also opens up new possibilities for *aggregation* in complex systems. We could model a complex system as a hybrid "meta-automaton", where the dynamics at each discrete meta-mode $p \in P$ are given by the reachability relation h_p of a (basic) hybrid automaton over state space $X_p \subseteq Q_p \times \mathbb{R}^n$, with switching relations from X_p to $X_{p'}$ between automata, as illustrated in Figure 2. We now have the machinery with which to formally reason about the dynamics of such a creature.

We also gain a clearer view of the enterprise of symbolic model checking for hybrid and real-time systems, as implemented in tools such as HyTech and Kronos. The basic task of such systems is to compute the *reachable region* of a hybrid dynamical system under the control of a given hybrid automaton $\mathcal{H}$. As noted in the recent paper of Henzinger, Kupferman and Qadeer [20], to capture the notion "reachable from φ", as distinct from "reaches φ", one needs in the semantics the *post-image*, rather than the pre-image, operator of a relation. The cleanest way to do it is to use the basic identity: $\mathrm{post}[r] = \mathrm{pre}[\breve{r}]$, where $\breve{r}$ is the relational *converse* or *inverse* of r, and to extend the μ-calculus with a converse operation governed by the rule:

$$\langle \breve{a}\rangle\psi \to \varphi \quad \text{iff} \quad \psi \to [a]\varphi \tag{9}$$

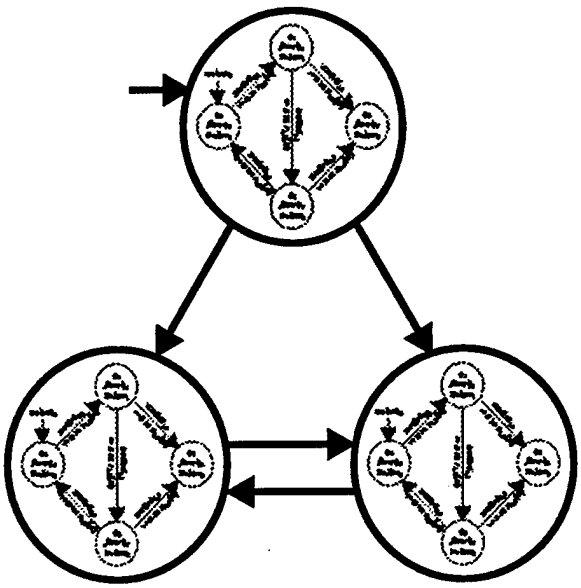

Fig. 2. Aggregation in complex systems

Then the sentence

$$\langle \breve{\mathbf{h}} \rangle \, \mathbf{Init} \tag{10}$$

denotes the reachable region, where the *post* modalities $\langle \breve{\mathbf{h}} \rangle$ and $[\breve{\mathbf{h}}]$ are defined as in (5), but substituting the converse relations. Symbolic model checking tools attempt to compute the *value* of $\| \langle \breve{\mathbf{h}} \rangle \, \mathbf{Init} \|^{\mathfrak{M}}$ as a *first-order formula* in $n+1$ free variables $(z, x_1, ..., x_n)$, in the language $\mathcal{L}(\overline{\mathbb{R}})$ of, say, the structure $\overline{\mathbb{R}} = (\mathbb{R}; <, +, -, \cdot, 0, 1, \{\bar{q}\}_{q \in Q})$ as the real closed field[2] plus discrete constants. The procedure computes a sequence of first-order formulas $\chi_0, \chi_1, ..., \chi_k, ...$ which are *translations* of the μ-calculus formulas forming the approximation sequence for $\langle \breve{\mathbf{h}} \rangle \, \mathbf{Init}$, with the translation starting from the explicit first-order definitions of the set *Init* and the relations e_q and $c_{q,q'}$. The procedure terminates at stage $k+1$ if the formula: $\chi_{k+1} \leftrightarrow \chi_k$ is provable in the first-order theory $Th(\overline{\mathbb{R}})$ of the relevant structure over $\mathbb{R}$, in which case the reachable region is defined by χ_k. The procedure is guaranteed to terminate when the model $\mathfrak{M} = \mathfrak{M}_{\mathcal{H}}$ has a *finite bisimulation quotient* $\mathfrak{M}^{\approx}$, where $\approx$ is an equivalence relation on $X \subseteq Q \times \mathbb{R}^n$ which *respects* each of the transition relations e_q and $c_{q,q'}$ and the

[2] The real closed field $\overline{\mathbb{R}}$ admits elimination of quantifiers, so all first-order formulas in the language are provably equivalent in the theory $Th(\overline{\mathbb{R}})$ to a *quantifier-free* formula. The definable subsets of $\mathbb{R}^n$ in $\overline{\mathbb{R}}$ are the *semi-algebraic* sets: finite unions of sets defined by equalities and inequalities over polynomials $f \in \mathbb{R}[X_1, ..., X_n]$ [14].

observation sets $Init_q$, Inv_q, $Grd_{q,q'}$. The recent work by Lafferriere, Pappas, Sastry and Yovine [27], [28], identifies a class of systems whose LTS models $\mathfrak{M}_{\mathcal{H}}$ are first-order definable in an *o-minimal structure* $\overline{\mathbb{R}}$ expanding the real-closed field. The finite cell decomposition property of such structures (together with a restriction on the form of the controlled jumps relations $c_{q,q'}$) is used to construct the finite bisimulation equivalence. (The theory of definable sets in o-minimal structures is developed in van den Dries' monograph *Tame Topology and O-minimal Structures* [14].)

The basic propositional modal μ-calculus can provide both a usable and a richly expressive formalism for reasoning about the *abstract dynamics* of hybrid systems. We want and need more. We want to be able to express in our logical formalisms what we *mean* by *continuous* and *discrete* dynamics, and hybrids of the two. We want to be able to formally express notions of *imprecision* or *metric tolerance*, such as the property of "being within distance ϵ" of a set, for a particular $\epsilon > 0$. More generally, we want a logical formalism that supports not only the specification and verification of single properties, but the larger task of representing and building up a *knowledge base* of properties of a system, starting with structural properties assumed in the modeling, and then adding new facts as they are verified by either model-checking or deductive means.

The remainder of this paper is an exploration of how the propositional modal μ-calculus can form a basis for a cohesive and expressively rich logical framework for the formal analysis of hybrid systems. In developing the logics, our key resources include:

1. *modal logics*, considered as a general formalism for reasoning about binary relations and operators on sets ([9], [35], [38], [5]); and
2. *set-valued analysis and dynamical systems theory*, brought into play by considering transition relations $r \subseteq X \times X$ in their equivalent form as *set-valued maps* $r : X \rightsquigarrow X$, i.e. functions $r : X \to \mathcal{P}(X)$ ([1], [6], [7]).

In the course of this paper, it will be important to keep an eye on both the distinction and the interplay between:

- the μ-calculus and various extensions as *propositional modal logics* (and thus ultimately *monadic second-order logics* [25]), in which formulas of the *same* formal language can be meaningfully interpreted in a variety of LTS models of any cardinality; in particular, in both continuum-sized models $\mathfrak{M}$ and in finite quotients $\mathfrak{M}^{\approx}$; and
- the *first-order* languages $\mathcal{L}(\overline{\mathbb{R}})$ and theories $Th(\overline{\mathbb{R}})$ of specific structures $\overline{\mathbb{R}} = (\mathbb{R}; <, +, -, \cdot, 0, 1, ...)$ over the reals, used in defining the components – the state space X, the transition relations $a^{\mathfrak{M}}$ and observation sets $||p||^{\mathfrak{M}}$ – of particular, albeit intended, LTS models $\mathfrak{M}$.

With regard to the latter, note that in the theory of o-minimal structures, relations $r : \mathbb{R}^m \rightsquigarrow \mathbb{R}^n$ go by the name of *definable families* $(r_x)_{x \in \mathbb{R}^m}$ ([14] §3.3).

To restate the point, the *system description* language is that of first-order logic, while the *system specification* language is that of propositional polymodal logic with fixed-point quantifiers.

This paper is one installment of a larger project. An analysis of the concept of bisimulation, and its relation to the algebraic semantics for the μ-calculus, is given in [11], and [12] gives the completeness of deductive proof systems for normal polymodal extensions of the μ-calculus. Related logics and earlier versions of some of the ideas are found in [10].

The paper is organized as follows. Section 2 is a review and analysis of basic hybrid systems and their associated LTS models. Section 3 is a review of the syntax and LTS semantics of the modal μ-calculus. In Section 4, we flesh out the skeleton of an LTS model by imbuing the state space with topological and metric tolerance structure; we explore continuity and tolerance properties of relations $r : X \rightsquigarrow Y$ and applications to components of hybrid automata. Section 5 presents deductive proof systems for the new logics, extending Kozen's axiomatization of $\mathbf{L}_\mu$. Section 6 is a brief discussion of ongoing research.

2 Basic hybrid automata and associated LTS models

First, a note on notation. For a set X, $\mathcal{P}(X)$ denotes the family of all subsets of X (a complete Boolean algebra). Following [6], the notation $r : X \rightsquigarrow Y$ means $r \subseteq X \times Y$ is a relation, or equivalently, $r : X \to \mathcal{P}(Y)$ is a set-valued map, with values $r(x) \subseteq Y$ for $x \in X$. The expressions:

$$x \xrightarrow{r} y, \quad (x, y) \in r, \quad y \in r(x) \text{ and } x\, r\, y$$

are synonymous. The *domain* of $r : X \rightsquigarrow Y$ is defined by $\mathrm{dom}(r) \triangleq \sigma(r)(Y)$, and the *range* $\mathrm{ran}(r) \triangleq \sigma(\breve{r})(X) = \mathrm{dom}(\breve{r})$. Relational compositions $r \cdot s$ of $r : X \rightsquigarrow Y$ and $s : Y \rightsquigarrow Z$ are read from left to right in sequential order, defined by:

$$x \xrightarrow{r \cdot s} z \quad \triangleq \quad (\exists y \in Y) \quad x \xrightarrow{r} y \text{ and } y \xrightarrow{s} z$$

(cf. [1] where composition is written in the reverse order, as for functional composition.)

We base our discussion on a generalization of the systems considered in [27],[28], depicted in Figure 1. Figure 3 is an illustration.

Definition 1. *A (basic, evolution time-deterministic)* hybrid system *is a structure*

$$\mathcal{H} = (Q, G, \{X_q\}_{q \in Q}, \{\phi_q\}_{q \in Q}, \{Init_q\}_{q \in Q}, \{Inv_q\}_{q \in Q}, \\ \{r_{q,q'}\}_{(q,q') \in G}, \{Grd_{q,q'}\}_{(q,q') \in G})$$

where

- Q *is a finite set of* discrete states *or* control modes*;*
- $G \subseteq Q \times Q$ *is the* control graph *of* discrete transitions*;*
- *for each* $q \in Q$*,*
  - $X_q \subseteq \mathbb{R}^n$ *is the state space for mode* q*;*
  - $\phi_q : X_q \times \mathbb{R}^+ \to X_q$ *is the continuous semi-flow of a vector field on* X_q*;*
  - $Inv_q \subseteq X_q$ *is the set of* invariant *states for mode* q*, or the* domain of permitted evolution *within mode* q*;*
  - $Init_q \subseteq Inv_q$ *is the set of* initial *states for mode* q *(possibly empty);*
- *for each discrete transition* $(q, q') \in G$*,*
  - $Grd_{q,q'} \subseteq X_q$ *is the* guard set *for the jump from* q *to* q'*;*
  - $r_{q,q'} : X_q \rightsquigarrow X_{q'}$ *is the* reset *relation;*
    for $x \in X_q$*,* $r_{q,q'}(x) \subseteq X_{q'}$ *is the set of possible reassignment states after the jump from* q *to* q'*.*

The *hybrid state space* of the system $\mathcal{H}$ is the set

$$X = \bigcup_{q \in Q} \{q\} \times X_q$$

To keep things simple, assume a fixed number n of real-valued coordinates, so $X_q \subseteq \mathbb{R}^n$ for each $q \in Q$. In [27],[28], the systems under consideration are simpler again in that they have *constant* reset relations $r_{q,q'} = Grd_{q,q'} \times Rst_{q,q'}$, with the constant set of reassignment states $Rst_{q,q'} \subseteq Inv_{q'}$.

The intention is that a hybrid system, so defined, is the *semantic content* of a hybrid automaton in the sense of Henzinger [19], Def. 1.1. For definiteness, we take a (basic, evolution time-deterministic) *hybrid automaton* to be a hybrid system $\mathcal{H}$ with a *concrete syntactic description*, namely:

- the discrete structure is given by a finite graph (Q, G), where $G \subseteq Q \times Q$;
- each of the component sets X_q, $Init_q$, Inv_q, $Grd_{q,q'} \subseteq \mathbb{R}^n$, semi-flows $\phi_q : X_q \times \mathbb{R}^+ \to X_q$, and reset relations $r_{q,q'} \subseteq X_q \times X_{q'}$ have explicit first-order definitions in the language $\mathcal{L}(<, +, -, \cdot, 0, 1, ...)$ of some specified structure $\overline{\mathbb{R}}$ over the reals.

From [27], [28], we have reason to want such a structure $\overline{\mathbb{R}}$ to be o-minimal.

Operationally, a hybrid automaton $\mathcal{H}$ can be thought of as defining a non-deterministic *hybrid control policy*, partially defined on states $(z, x) \in X$:

if $z = q$ and $x \in Inv_q$
then **stay** in discrete mode q and **continue** evolution according to ϕ_q;
if $z = q$ and $x \in Grd_{q,q'}$ for some $(q, q') \in G$,
then **switch** to discrete mode q', **re-initialize** to some $x' \in r_{q,q'}(x)$,
and then evolve according to the flow $\phi_{q'}$.

The *domain of definition* of $\mathcal{H}$ is given by:

$$\mathrm{dom}(\mathcal{H}) \triangleq \left(\bigcup_{q \in Q} \{q\} \times Inv_q\right) \cup \left(\bigcup_{(q,q') \in G} \{q\} \times Grd_{q,q'}\right)$$

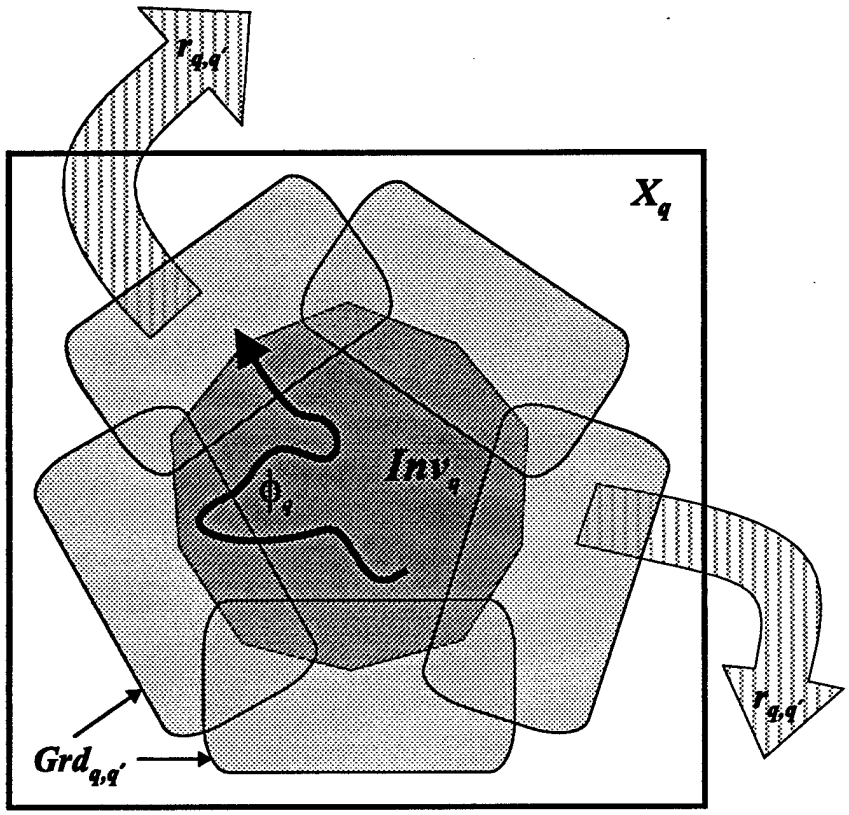

Fig. 3. Operation of basic hybrid automaton

If $z = q$ and $x \in Grd_{q,q'}$ for some $(q, q') \in G$, then that discrete control switch is said to be *enabled*; if $(q, x) \in \mathrm{dom}(\mathcal{H})$ but $x \notin Inv_q$, then some discrete control switch is said to be *forced*. It is generally assumed that $r_{q,q'}(x) \subseteq Inv_{q'}$ for all $x \in Grd_{q,q'}$; in words, $Inv_{q'}$ is (forward) $r_{q,q'}$-invariant from $Grd_{q,q'}$. In some expositions (e.g. [27]), it is required that $\mathcal{H}$ be *total* or *non-blocking*, which amounts to the assumption that $\mathrm{dom}(\mathcal{H}) = X$.

In descriptions of the operation of a hybrid automaton and the ensuing class of trajectories of the system, it is generally assumed (e.g. [19]) that the state $x = (x_1, ..., x_n) \in \mathbb{R}^n$ of the physical plant is being *continuously sensed*, with *perfect precision*, and that the action and effect of a discrete control switch is *instantaneous*.

The accepted ([19], [27]) definition of the ("time-abstract") transition system of a hybrid automaton, with modified notation, is as follows.

Definition 2. *Given a hybrid system $\mathcal{H}$, the LTS model $\mathfrak{M}_{\mathcal{H}}$ determined by $\mathcal{H}$ has the following components:*

- *the state space* $X \triangleq \cup_{q \in Q} \{q\} \times X_q$;

– *for each discrete state* $q \in Q$, *the* constrained evolution *relation* $e_q : X_q \rightsquigarrow X_q$ *defined by:*

$$x \xrightarrow{e_q} x' \quad \triangleq \quad (\exists t \in \mathbb{R}^+)[\ x' = \phi_q(x,t)\ \wedge\ (\forall s \in [0,t])\ \phi_q(x,s) \in Inv_q\ ]$$

– *for each discrete transition* $(q,q') \in G$, *the* controlled jump *relation* $c_{q,q'} : X_q \rightsquigarrow X_{q'}$ *defined by:*

$$x \xrightarrow{c_{q,q'}} x' \quad \triangleq \quad x \in Grd_{q,q'}\ \wedge\ x' \in Inv_{q'}\ \wedge\ x \xrightarrow{r_{q,q'}} x'$$

– *the observation sets* X_q, $Init_q$, Inv_q, $Grd_{q,q'}$.

We adopt the notational convention of identifying, when convenient, sets $A_q \subseteq X_q$ and $\{q\} \times A_q \subseteq X$; moreover, the relations $e_q : X_q \rightsquigarrow X_q$ and $c_{q,q'} : X_q \rightsquigarrow X_{q'}$ can be "lifted" to relations $X \rightsquigarrow X$ in the obvious way.

From the definition of the evolution relation e_q, a desired property of the domain of evolution Inv_q is that it be *convex* with respect to the semi-flow ϕ_q, in the sense that:

$$\begin{array}{l}\text{if } x \in Inv_q \text{ and } \phi_q(x,t) \in Inv_q \text{ for some } t \geq 0,\\ \text{then } \phi_q(x,s) \in Inv_q \text{ for all } s \in [0,t]\end{array}$$

So no curve segment of the semi-flow with both endpoints in Inv_q ever leaves Inv_q at an intermediate point.

In the terminology of [1] Ch. 6, Definition 6.3, the (positive) *orbit relation* $f : X \rightsquigarrow X$ of a semi-flow $\phi : X \times \mathbb{R}^+ \to X$ is defined by:

$$x \xrightarrow{f} x' \quad \triangleq \quad (\exists t \in \mathbb{R}^+)\ \ x' = \phi(x,t) \tag{11}$$

With respect to the orbit relation $f_q : X_q \rightsquigarrow X_q$ of ϕ_q, the desired convexity property for Inv_q has the form:

$$\text{if } x_0, x_1 \in Inv_q \text{ and } x_0 \xrightarrow{f_q} x \xrightarrow{f_q} x_1 \text{ then } x \in Inv_q$$

So when Inv_q if f_q-convex, we have the decompositions

$$e_q = f_q \cap (Inv_q \times Inv_q) \quad \text{and} \quad c_{q,q'} = r_{q,q'} \cap (Grd_{q,q'} \times Inv_{q'})$$

in which case we may as well assume the LTS model $\mathfrak{M}_{\mathcal{H}}$ includes the (unconstrained) orbit relations f_q and the uncontrolled reset relation $r_{q,q'}$. If we want to express properties which require *both* the orbit relation f_q and its converse (convexity is one such), then we should include $\breve{f}_q$ as a component of $\mathfrak{M}_{\mathcal{H}}$ as well (see also [20]).

The modularity of the modal μ-calculus allows us to succinctly express not only *desired properties* – i.e. those to be verified, but also various of the structural properties of the LTS model $\mathfrak{M}_{\mathcal{H}}$ that it will typically possess *by assumption*. In

a deductive framework, such sentences and sentence schemes (formulas with free propositional variables Z) provide an initial stock of facts known to be true in the model, and serve as hypotheses in application of inference rules when seeking to expand one's stock of knowledge.

[1] $\langle \breve{\mathbf{f}}_q \rangle \mathbf{Inv}_q \wedge \langle \mathbf{f}_q \rangle \mathbf{Inv}_q \rightarrow \mathbf{Inv}_q$

[2] $\mathbf{Init}_q \rightarrow \mathbf{Inv}_q$

[3] $\mathbf{Init} \leftrightarrow \bigvee_{q \in Q} \mathbf{Init}_q$

[4] $\mathbf{Inv} \leftrightarrow \bigvee_{q \in Q} \mathbf{Inv}_q$

[5] $\langle \breve{\mathbf{r}}_{q,q'} \rangle \mathbf{Grd}_{q,q'} \rightarrow \mathbf{Inv}_{q'}$

[6] $\mathbf{Grd}_{q,q'} \rightarrow \langle \mathbf{r}_{q,q'} \rangle \mathbf{tt}$

[7] $\langle \mathbf{e}_q \rangle Z \leftrightarrow \mathbf{Inv}_q \wedge \langle \mathbf{f}_q \rangle (Z \wedge \mathbf{Inv}_q)$

[8] $\langle \breve{\mathbf{e}}_q \rangle Z \leftrightarrow \mathbf{Inv}_q \wedge \langle \breve{\mathbf{f}}_q \rangle (Z \wedge \mathbf{Inv}_q)$

[9] $\langle \mathbf{c}_{q,q'} \rangle Z \leftrightarrow \mathbf{Grd}_{q,q'} \wedge \langle \mathbf{r}_{q,q'} \rangle (Z \wedge \mathbf{Inv}_{q'})$

[10] $\langle \breve{\mathbf{c}}_{q,q'} \rangle Z \leftrightarrow \mathbf{Inv}_{q'} \wedge \langle \breve{\mathbf{r}}_{q,q'} \rangle (Z \wedge \mathbf{Grd}_{q,q'})$

[11] $\langle \mathbf{f} \rangle Z \leftrightarrow \bigvee_{q \in Q} \langle \mathbf{f}_q \rangle Z$

[12] $Z \rightarrow \langle \mathbf{f} \rangle Z$

[13] $\langle \mathbf{f}_q \rangle \langle \mathbf{f}_q \rangle Z \rightarrow \langle \mathbf{f}_q \rangle Z$

[14] $\langle \mathbf{e} \rangle Z \leftrightarrow \bigvee_{q \in Q} \langle \mathbf{e}_q \rangle Z$

[15] $\langle \mathbf{c} \rangle Z \leftrightarrow \bigvee_{(q,q') \in G} \langle \mathbf{c}_{q,q'} \rangle Z$

[16] $\langle \mathbf{h} \rangle \mathbf{tt} \leftrightarrow \bigvee_{q \in Q} \mathbf{Inv}_q \vee \bigvee_{(q,q') \in G} \mathbf{Grd}_{q,q'}$

[1] says that Inv_q is f_q-convex. [2] is merely that $Init_q \subseteq Inv_q$. [3] and [4] define the global initial and invariant sets. [5] is the assumption that $Inv_{q'}$ is (future) $r_{q,q'}$-invariant from $Grd_{q,q'}$. [6] says that every point in $Grd_{q,q'}$ has an $r_{q,q'}$-successor; i.e. $Grd_{q,q'} \subseteq \mathrm{dom}(r_{q,q'})$. [7] – [10] follow from the decompositions $e_q = f_q \cap (Inv_q \times Inv_q)$ and $c_{q,q'} = r_{q,q'} \cap (Grd_{q,q'} \times Inv_{q'})$. In particular, using the rule for converse (9) in Section 1 above, we have:

$$\varphi \rightarrow [\mathbf{e}_q]\varphi \quad \text{iff} \quad \mathbf{Inv}_q \wedge \langle \breve{\mathbf{f}}_q \rangle (\varphi \wedge \mathbf{Inv}_q) \rightarrow \varphi \tag{12}$$

and

$$\varphi \rightarrow [\mathbf{c}_{q,q'}]\varphi \quad \text{iff} \quad \mathbf{Inv}_{q'} \wedge \langle \breve{\mathbf{r}}_{q,q'} \rangle (\varphi \wedge \mathbf{Grd}_{q,q'}) \rightarrow \varphi \tag{13}$$

[11] defines f as the union of the orbit relations f_q. From the zero semi-flow property, each f_q is reflexive on its domain X_q, so f is reflexive (and total) on the whole space X, which is [12]. From the sum semi-flow property, each f_q is transitive; this is [13]. [14] and [15] are the definitions $e \triangleq \cup_{q \in Q} e_q$ and $c \triangleq \cup_{(q,q') \in G} c_{q,q'}$. From [7], [14] and [12], it follows that:

$$(Z \wedge \mathbf{Inv}) \rightarrow \langle \mathrm{e} \rangle (Z \wedge \mathbf{Inv}) \tag{14}$$

that is, the relational sum e is reflexive on its domain. And from [7] and [13], we get:

$$\langle \mathrm{e}_q \rangle \langle \mathrm{e}_q \rangle Z \rightarrow \langle \mathrm{e}_q \rangle Z \tag{15}$$

which says each e_q is transitive.

[16] defines the domain $\mathrm{dom}(\mathcal{H})$. The definitions of $\langle \mathbf{h} \rangle$ and $[\mathbf{h}]$ in (5) above should also be added to the list.

Using convexity assumption [1] and (12), the invariance assumption [5] and (13), and the invariance rule (7), it follows that $\mathbf{Inv} \rightarrow [\mathbf{h}]\,\mathbf{Inv}$ will be true in $\mathfrak{M}_{\mathcal{H}}$; i.e. the set Inv is future-invariant under $\mathcal{H}$. More generally, whenever $\mathbf{Inv} \rightarrow \varphi$ is true in $\mathfrak{M}_{\mathcal{H}}$, then $\mathbf{Init} \rightarrow [\mathbf{h}]\,\varphi$ will be true, and thus on the current interpretation, $\|\varphi\|^{\mathfrak{M}}$ is *safe* under the action of $\mathcal{H}$, since no (perfect precision) hybrid trajectory starting in $Init$ *ever leaves* Inv. So in this scenario, the situation of a controlled jump being *forced* – that is, $(q, x) \in \mathrm{dom}(\mathcal{H})$ but $x \notin Inv_q$ – can in fact never arise. Perfect precision trajectories start or land inside Inv_q, evolve continuously according to ϕ_q, and then while the state is still *inside* Inv_q, or at worst on the (topological) *boundary* of Inv_q, a jump is made according to $c_{q,q'}$.

In some accounts of the LTS model of a hybrid automata (including that in [19]), the definition of the constrained evolution relation e_q is slightly weaker, with the requirement: $\forall s \in [0,t), \quad \phi_q(x,s) \in Inv_q$, so the end-point $\phi_q(x,t)$ need not lie in Inv_q. If Inv_q is *closed* (in the standard topology on $X_q \subseteq \mathbb{R}^n$), then the continuity of $\phi_q : X_q \times \mathbb{R}^+ \rightarrow X_q$ entails that all such end-points *will* lie in Inv_q regardless, so the weakening makes no difference. In virtually all concrete examples of hybrid automata in the literature, the invariant sets Inv_q are closed.

In Section 4, when we adjoin modalities corresponding to the interior and closure operators of a topology, we will be able to formally express properties such as being open, closed, or the topological boundary of a set. We will also be able to give formal expression to the assumption that the orbit relations f_q are those of *continuous* semi-flows, and to consider consequences of continuity.

We also clearly need to entertain the possibility that a physical realization of a hybrid automaton as a control policy might be *less than perfect*: sensors will be accurate only up to some level of precision; we should allow for delay between sensing the state and acting on that sensor reading in accordance with the control policy; and then there are margins of error in real-valued constants used in first-order definitions of the components of the model. In Section 4, we will consider alternative classes of hybrid trajectories by playing with the definitions of the fixed-point modalities $\langle \mathbf{h} \rangle$ and $[\mathbf{h}]$ in an enriched modal language containing

modalities $\langle\epsilon\rangle$ and $[\epsilon]$ interpreted by metric ϵ-tolerance relations, for concrete values of $\epsilon > 0$.

3 Syntax and LTS semantics of the modal μ-calculus

The μ-calculus originated in the late 1960's (Scott and de Bakker) as a formal logic of digital programs, the input-output behavior of an atomic program being represented as a binary transition relation on (discrete) states. Contemporary introductions to the μ-calculus can be found in [38], [15]. In this section, we review the syntax and semantics over LTS models of the propositional modal μ-calculus.

Definition 3. *A* modal signature *is a pair (Φ, Σ), where Φ is a set of* propositional constants *and Σ is a set of* transition labels. *Let* PVar *denote a fixed set of propositional (second-order or set-valued) variables. The collection $\mathcal{F}_\mu(\Phi, \Sigma)$ of* formulas *of the propositional modal μ-calculus is generated by the grammar:*

$$\varphi ::= \mathbf{ff} \mid p \mid Z \mid \neg\varphi \mid \varphi_1 \vee \varphi_2 \mid \langle a\rangle\varphi \mid \mu Z.\varphi$$

for propositional constants $p \in \Phi$, propositional variables $Z \in$ PVar, and transition labels $a \in \Sigma$, and with the proviso that in $\mu Z.\varphi$, the variable Z occur positively, *i.e. each occurrence of Z in φ is within the scope of an even number of negations.*

The other (classical) propositional connectives, modalities and greatest fixed point quantifier are defined in the usual way:

$$\begin{aligned} \mathbf{tt} &\triangleq \neg\mathbf{ff} & \varphi_1 \wedge \varphi_2 &\triangleq \neg(\neg\varphi_1 \vee \neg\varphi_2) \\ \varphi_1 \to \varphi_2 &\triangleq \neg\varphi_1 \vee \varphi_2 & \varphi_1 \leftrightarrow \varphi_2 &\triangleq (\varphi_1 \to \varphi_2) \wedge (\varphi_2 \to \varphi_1) \\ [a]\varphi &\triangleq \neg\langle a\rangle\neg\varphi & \nu Z.\varphi &\triangleq \neg\mu Z.\neg\varphi[Z := \neg Z] \end{aligned}$$

An occurrence of a variable $Z \in$ PVar in a formula that is within the scope of a μZ is called *bound*, otherwise it is *free* (as in first-order logic). Let $\mathcal{S}_\mu(\Phi, \Sigma)$ denote the set of all *sentences*, or closed formulas of $\mathcal{F}_\mu(\Phi, \Sigma)$, i.e. those without any free variables, and let $\mathcal{F}(\Phi, \Sigma)$ and $\mathcal{S}(\Phi, \Sigma)$ denote, respectively, the set of all purely *modal* formulas and sentences, i.e. those containing no fixed point quantifiers, and in case of sentences, no variables Z.

For formulas $\varphi, \psi \in \mathcal{F}_\mu(\Phi, \Sigma)$, let $\varphi[Z := \psi]$ denote the result substituting ψ for all free occurrences of Z. By renaming bound variables in φ if necessary, we can assume such substitutions do not result in the unintended capture of free variables.

Definition 4. *Given an LTS $\mathfrak{M} = (X, \{a^{\mathfrak{M}}\}_{a\in\Sigma}, \{\|p\|^{\mathfrak{M}}\}_{p\in\Phi})$ of modal signature (Φ, Σ), a (propositional, or second-order)* variable assignment *in $\mathfrak{M}$ is any*

map $\xi : \mathrm{PVar} \to \mathcal{P}(X)$. *Each such assignment* ξ *uniquely extends to a* denotation *map* $\|\cdot\|^{\mathfrak{M}}_{\xi} : \mathcal{F}_{\mu}(\Phi, \Sigma) \to \mathcal{P}(X)$ *as follows:*

$$\begin{aligned}
\|\mathbf{ff}\|^{\mathfrak{M}}_{\xi} &\doteq \varnothing \\
\|p\|^{\mathfrak{M}}_{\xi} &\doteq \|p\|^{\mathfrak{M}} && \text{for } p \in \Phi \\
\|Z\|^{\mathfrak{M}}_{\xi} &\doteq \xi(Z) && \text{for } Z \in \mathrm{PVar} \\
\|\neg\varphi\|^{\mathfrak{M}}_{\xi} &\doteq X - \|\varphi\|^{\mathfrak{M}}_{\xi} \\
\|\varphi_1 \vee \varphi_2\|^{\mathfrak{M}}_{\xi} &\doteq \|\varphi_1\|^{\mathfrak{M}}_{\xi} \cup \|\varphi_2\|^{\mathfrak{M}}_{\xi} \\
\|\langle a\rangle\varphi\|^{\mathfrak{M}}_{\xi} &\doteq \sigma(a^{\mathfrak{M}})\left(\|\varphi\|^{\mathfrak{M}}_{\xi}\right) && \text{for } a \in \Sigma \\
\|\mu Z.\varphi\|^{\mathfrak{M}}_{\xi} &\doteq \bigcap\{A \in \mathcal{P}(X) \mid \|\varphi\|^{\mathfrak{M}}_{\xi(A/Z)} \subseteq A\}
\end{aligned}$$

where the pre-image operator $\sigma(a^{\mathfrak{M}})$ *is defined as in* (2) *above, and for sets* $A \in \mathcal{P}(X)$, *the variant assignment* $\xi(A/Z) : \mathrm{PVar} \to \mathcal{P}(X)$ *is given by:*

$$\xi(A/Z)(W) = \xi(W) \text{ if } W \neq Z, \quad \text{and} \quad \xi(A/Z)(W) = A \text{ if } W = Z.$$

For formulas $\varphi \in \mathcal{F}_{\mu}(\Phi, \Sigma)$ *and assignments* $\xi : \mathrm{PVar} \to \mathcal{P}(X)$ *in* $\mathfrak{M}$, *we say:*

- φ *is* true at state x *in* $(\mathfrak{M}, \xi)$, *written:* $\mathfrak{M}, \xi, x \models \varphi$, *iff* $x \in \|\varphi\|^{\mathfrak{M}}_{\xi}$;
- φ *is* true *in* $(\mathfrak{M}, \xi)$, *written:* $\mathfrak{M}, \xi \models \varphi$, *iff* $\|\varphi\|^{\mathfrak{M}}_{\xi} = X$; *i.e.* φ *is true at all states* x *in* $(\mathfrak{M}, \xi)$; *and*
- φ *is* true *in* $\mathfrak{M}$, *written:* $\mathfrak{M} \models \varphi$, *iff* φ *is true in* $(\mathfrak{M}, \xi)$ *for* all *assignments* ξ *in* $\mathfrak{M}$.

For sentences $\varphi \in \mathcal{S}_{\mu}(\Phi, \Sigma)$, the denotation $\|\varphi\|^{\mathfrak{M}}_{\xi}$ is independent of the variable assignment ξ, and is written $\|\varphi\|^{\mathfrak{M}}$. So $\mathfrak{M} \models \varphi$ iff $\mathfrak{M}, \xi \models \varphi$ for *any* assignment ξ.

Given a model $\mathfrak{M}$ and variable assignment ξ, each formula $\varphi \in \mathcal{F}_{\mu}(\Phi, \Sigma)$ and each variable $Z \in \mathrm{PVar}$ free in φ, together determine an operator on sets $\varphi^{\mathfrak{M}}_{\xi,Z} : \mathcal{P}(X) \to \mathcal{P}(X)$ given by:

$$\left(\varphi^{\mathfrak{M}}_{\xi,Z}\right)(A) \doteq \|\varphi\|^{\mathfrak{M}}_{\xi(A/Z)} \tag{16}$$

The variant assignment construct corresponds to substitution: for all formulas $\psi \in \mathcal{F}_{\mu}(\Phi, \Sigma)$,

$$\left(\varphi^{\mathfrak{M}}_{\xi,Z}\right)\left(\|\psi\|^{\mathfrak{M}}_{\xi}\right) = \|\varphi[Z := \psi]\|^{\mathfrak{M}}_{\xi} \tag{17}$$

When the variable Z occurs positively within φ, so $\mu Z.\varphi \in \mathcal{F}_{\mu}(\Phi, \Sigma)$, the operator $\varphi^{\mathfrak{M}}_{\xi,Z}$ is $\subseteq$-monotone:

$$A \subseteq B \quad \Rightarrow \quad F(A) \subseteq F(B)$$

for $F = \varphi^{\mathfrak{M}}_{\xi,Z}$. The clause in Definition 4 for μ-formulas says that $\|\mu Z.\varphi\|^{\mathfrak{M}}_{\xi}$ is the $\subseteq$-*least pre-fixed-point* of the monotone operator $\varphi^{\mathfrak{M}}_{\xi,Z}$ in the complete lattice $\mathcal{P}(X)$. So by the Tarski-Knaster fixed-point theorem, $\|\mu Z.\varphi\|^{\mathfrak{M}}_{\xi}$ must also be the $\subseteq$-*least fixed-point* of $\varphi^{\mathfrak{M}}_{\xi,Z}$; that is:

$$\|\mu Z.\varphi\|^{\mathfrak{M}}_{\xi} = \bigcap\{A \in \mathcal{P}(X) \mid \|\varphi\|^{\mathfrak{M}}_{\xi(A/Z)} = A\}$$

In the standard set-theoretic semantics for the μ-calculus, as presented here and given in [23], [38], [40], [15], the propositional variables Z range over the full power-set (and complete Boolean algebra) $\mathcal{P}(X)$ – that is, *all* subsets of X. An alternative, developed by Kwiatkowska and colleagues [5], [8], is an *algebraic semantics* in which the range of propositional variables is restricted to a *subfamily* $\mathcal{A} \subseteq \mathcal{P}(X)$. This work has roots in a number of classic studies from the 1950's, notably that of Henkin [18] on completeness of higher-order logic; of Jónsson and Tarski [26] on Boolean algebras with operators; and that of Rasiowa and Sikorski [36] on algebraic logic.

Definition 5. ([5], [8]). *Given an LTS model $\mathfrak{M}$, a family of sets $\mathcal{A} \subseteq \mathcal{P}(X)$ is said to be a* modal algebra *for $\mathfrak{M}$, and the pair $(\mathfrak{M}, \mathcal{A})$ is known as a* modal frame, *when each of the following holds:*

1. *$\mathcal{A}$ contains each of the observation sets $\|p\|^{\mathfrak{M}}$, for $p \in \Phi$;*
2. *$\mathcal{A}$ is a Boolean algebra under the finitary set-theoretic operations; and*
3. *$\mathcal{A}$ is closed under each of the pre-image operators $\sigma(a^{\mathfrak{M}})$ and $\tau(a^{\mathfrak{M}})$, for $a \in \Sigma$.*

For purely modal formulas $\varphi \in \mathcal{F}(\Phi, \Sigma)$, *the clauses in the inductive definition of the denotation $\|\varphi\|^{\mathcal{A}}_{\xi} \subseteq X$ with respect to a modal frame $(\mathfrak{M}, \mathcal{A})$ are identical to those in Definition 4 for $\|\varphi\|^{\mathfrak{M}}_{\xi}$, with the proviso that variable assignments ξ are* restricted *to $\mathcal{A}$, i.e. $\xi : \mathrm{PVar} \to \mathcal{A}$.*

A formula φ is true in the frame $(\mathfrak{M}, \mathcal{A})$, written $(\mathfrak{M}, \mathcal{A}) \models \varphi$, iff $\|\varphi\|^{\mathcal{A}}_{\xi} = X$ for all assignments ξ in $\mathcal{A}$.

An LTS model $\mathfrak{M}$ is identified with the modal frame $(\mathfrak{M}, \mathcal{P}(X))$.

Modal algebras $\mathcal{A} \subseteq \mathcal{P}(X)$ need not be complete as lattices, so unlike $\mathcal{P}(X)$, we have no guarantee that the set being the $\subseteq$-least pre-fixed-point of $\varphi^{\mathcal{A}}_{\xi,Z}$ in fact exists in $\mathcal{A}$; when it does, it is the least fixed-point in $\mathcal{A}$ of $\varphi^{\mathcal{A}}_{\xi,Z}$, by a variant of the argument in the Tarski-Knaster fixed-point theorem.

Definition 6. ([5], [8]). *A modal algebra $\mathcal{A} \subseteq \mathcal{P}(X)$ is called a* modal μ-algebra, *and the pair $(\mathfrak{M}, \mathcal{A})$ called a* modal μ-frame, *if for each formula $\mu Z.\varphi \in \mathcal{F}_{\mu}(\Phi, \Sigma)$ the infinitary meet or infimum of the family in $\mathcal{A}$ of pre-fixed-points of $\varphi^{\mathcal{A}}_{\xi,Z}$*

$$\bigwedge\{A \in \mathcal{A} \mid \|\varphi\|^{\mathcal{A}}_{\xi(A/Z)} \subseteq A\}$$

exists in $\mathcal{A}$, in which case $\|\mu Z.\varphi\|^{\mathcal{A}}_{\xi}$ is that set.

In general, the denotations $\|\varphi\|^{\mathfrak{M}}_{\xi}$ and $\|\varphi\|^{\mathcal{A}}_{\xi}$ part company on μ-formulas, since the smallest of *all sets* $A \in \mathcal{P}(X)$ such that a condition holds will be contained in the smallest of all sets $A \in \mathcal{A}$ for which the same condition holds. In [11], we identify conditions under which a modal μ-frame $(\mathfrak{M}, \mathcal{A})$ is in *semantic agreement* with $\mathfrak{M}$, i.e. for all μ-formulas $\varphi \in \mathcal{F}_{\mu}(\Phi, \Sigma)$, $\|\varphi\|^{\mathcal{A}}_{\xi} = \|\varphi\|^{\mathfrak{M}}_{\xi}$ for all assignments ξ restricted to $\mathcal{A}$. The *smallest* μ-algebra for an LTS $\mathfrak{M}$ is the countable algebra

$$\mathcal{S}^{\mathfrak{M}}_{\mu} \triangleq \{\, \|\varphi\|^{\mathfrak{M}} \mid \varphi \in \mathcal{S}_{\mu}(\Phi, \Sigma) \,\}$$

of denotations of μ-sentences in $\mathfrak{M}$. It is readily verified that $\mathcal{S}^{\mathfrak{M}}_{\mu}$ is in semantic agreement $\mathfrak{M}$.

From the purely modal clauses in Definition 4, together with the definitions of the pre-image operators in (2), it follows that if the state space, transition relations and observation sets of an LTS model $\mathfrak{M}$ are all first-order definable in some structure, then for all *modal* sentences $\varphi \in \mathcal{S}(\Phi, \Sigma)$, the denotation $\|\varphi\|^{\mathfrak{M}} \subseteq X$ is first-order definable. Otherwise put, the countable algebra

$$\mathcal{S}^{\mathfrak{M}} \triangleq \{\, \|\varphi\|^{\mathfrak{M}} \mid \varphi \in \mathcal{S}(\Phi, \Sigma) \,\}$$

of denotations in $\mathfrak{M}$ of purely modal sentences, has a *finitary syntactic representation* as a family of first-order formulas; a family finitely generated by the explicit first-order definitions of the components of $\mathfrak{M}$, under the straight-forward translation of modal sentences based on the definitions (2) and the (classical) meaning of the Boolean connectives. Of course, an optimal situation is when the first-order structure admits *quantifier-elimination*, as then the naive translation of a modal sentence can be reduced to a quantifier-free formula, and so the algebra $\mathcal{S}^{\mathfrak{M}}$ will have a simpler and more tractable representation. Such algebras are the semantic content of Henzinger's notion of a *symbolic execution theory* in [19] §3.1.

Returning to the standard set-theoretic semantics, the completeness of $\mathcal{P}(X)$ as lattice ensures that the set $\|\mu Z.\varphi\|^{\mathfrak{M}}_{\xi}$ has an equivalent characterization (by the Park-Hitchcock fixed-point theorem) as the union of an $\subseteq$-increasing sequence of approximations:

$$\|\mu Z.\varphi\|^{\mathfrak{M}}_{\xi} = \bigcup_{\alpha < Ord(\mathfrak{M})} \|\varphi\|^{\mathfrak{M}}_{\xi,\alpha}$$

where

$$\begin{aligned}
\|\varphi\|^{\mathfrak{M}}_{\xi,0} &\triangleq \varnothing \\
\|\varphi\|^{\mathfrak{M}}_{\xi,\alpha+1} &\triangleq \varphi^{\mathfrak{M}}_{\xi,Z}\left(\|\varphi\|^{\mathfrak{M}}_{\xi,\alpha}\right) \\
\|\varphi\|^{\mathfrak{M}}_{\xi,\eta} &\triangleq \bigcup_{\alpha<\eta} \|\varphi\|^{\mathfrak{M}}_{\xi,\alpha} \qquad \text{for limit ordinals } \eta
\end{aligned}$$

and $Ord(\mathfrak{M}) < \kappa^+$, for $\kappa = Card(X)$, is the closure ordinal of $\mathfrak{M}$. The sets $\|\varphi\|^{\mathfrak{M}}_{\xi,\alpha}$ are μ-approximations of $\|\mu Z.\varphi\|^{\mathfrak{M}}_{\xi}$. Likewise, the denotation of $\nu Z.\varphi$ can be represented as the intersection of an $\subseteq$-decreasing sequence of ν-approximations.

In the general case, over LTS models $\mathfrak{M}$ of arbitrary cardinality, approximation sequences for the denotation of fixed-point formulas proceed through transfinite ordinals; when X has the cardinality of the continuum, $Ord(\mathfrak{M})$ could be much longer than we care to deal with.

When the operator $\varphi^{\mathfrak{M}}_{\xi,Z}$ corresponding to the body of a μ-formula $\mu Z.\varphi$ is *ω-chain-additive*, that is, for $F = \varphi^{\mathfrak{M}}_{\xi,Z}$

$$F\left(\bigcup_{n<\omega} A_n\right) = \bigcup_{n<\omega} F(A_n) \quad \text{where } A_n \subseteq A_{n+1} \text{ for all } n < \omega$$

then the ordinal of convergence for $\|\mu Z.\varphi\|^{\mathfrak{M}}_{\xi}$ is at worst ω. In this case, we have a sequence of approximation formulas

$$\varphi^0 \doteq \mathbf{ff} \quad \text{and} \quad \varphi^{n+1} \doteq \varphi[Z := \varphi^n] \quad \text{for } n < \omega \tag{18}$$

and

$$\|\mu Z.\varphi\|^{\mathfrak{M}}_{\xi} = \bigcup_{n<\omega} \|\varphi^n\|^{\mathfrak{M}}_{\xi}$$

since $\|\varphi^n\|^{\mathfrak{M}}_{\xi} = \|\varphi\|^{\mathfrak{M}}_{\xi,n}$. The terms "order-continuous" and "continuous from below" are also used instead of ω-chain-additive, since such an $F : \mathcal{P}(X) \to \mathcal{P}(X)$ is a continuous function with respect to the *Scott topology* on the complete partial order $(\mathcal{P}(X), \subseteq)$. We adapt the terminology of Jónsson and Tarski [26] on Boolean algebras with operators, since we are interested in other meanings of "continuous". Dually, when $\varphi^{\mathfrak{M}}_{\xi,Z}$ is *ω-chain-multiplicative*, the ordinal of convergence for $\|\nu Z.\varphi\|^{\mathfrak{M}}_{\xi}$ is at worst ω, and the sequence of approximation formulas starts at $\mathbf{tt}$ and decreases.

In particular, the semantic operator corresponding to the body of $\langle \mathbf{h} \rangle \varphi$ (or $\langle \breve{\mathbf{h}} \rangle \varphi$), as defined in (5), for sentences φ, is:

$$A \longmapsto \sigma(e)(\|\varphi\|^{\mathfrak{M}}) \cup \sigma(ec)(A)$$

Since the $\exists$-pre-image of any relation is *completely additive*, i.e. distributes over arbitrary unions, it follows that $\|\langle \mathbf{h} \rangle \varphi\|^{\mathfrak{M}}$ is the union of the denotations of the approximation sequence

$$\mathbf{ff}, \quad \langle \mathbf{e} \rangle \varphi, \quad \langle \mathbf{e} \rangle \varphi \vee \langle \mathbf{e} \rangle \langle \mathbf{c} \rangle \langle \mathbf{e} \rangle \varphi, \quad \langle \mathbf{e} \rangle \varphi \vee \langle \mathbf{e} \rangle \langle \mathbf{c} \rangle \langle \mathbf{e} \rangle \varphi \vee \langle \mathbf{e} \rangle \langle \mathbf{c} \rangle \langle \mathbf{e} \rangle \langle \mathbf{c} \rangle \langle \mathbf{e} \rangle \varphi, \ \ldots$$

Dually, the semantic operator corresponding to $[\mathbf{h}]$ is *completely multiplicative.*

When $\approx$ is a *bisimulation equivalence* on $\mathfrak{M}$ – that is, an equivalence relation on X which *respects* the transition relations $a^{\mathfrak{M}}$ and the observation sets $\|p\|^{\mathfrak{M}}$

in a suitable sense[3] – then the fundamental property of truth-preservation is as follows: for all sentences $\varphi \in \mathcal{S}_\mu(\Phi, \Sigma)$ and all $x, y \in X$,

$$x \approx y \quad \Rightarrow \quad [\ x \in \|\varphi\|^{\mathfrak{M}} \ \Leftrightarrow \ y \in \|\varphi\|^{\mathfrak{M}}\ ] \tag{19}$$

It follows that if $\approx$ is a bisimulation equivalence of *finite* index N, then the denotation $\|\varphi\|^{\mathfrak{M}}$ of each sentence is a *finite* union of equivalence classes under $\approx$. Hence for sentences $\mu Z.\varphi$ and $\nu Z.\varphi$, the ordinal of convergence for $\|\mu Z.\varphi\|^{\mathfrak{M}}$ and $\|\nu Z.\varphi\|^{\mathfrak{M}}$ is bounded by N. In this case, the finite quotient LTS $\mathfrak{M}^{\approx}$ is a finite simulacrum, and finite automaton representation, of the original system $\mathfrak{M}$. If such is the case, the countable μ-algebra $\mathcal{S}_\mu^{\mathfrak{M}}$ is in fact a *finite* algebra, and the atoms of the algebra are the equivalence classes under $\approx$. The familiar *bisimulation algorithm* ([19] §3.1; [27] §2) can be reinterpreted algebraically as the construction of a sequence of algebras $\mathcal{S}_k^{\mathfrak{M}}$ for $k < \omega$, where

$$\mathcal{S}_k^{\mathfrak{M}} \triangleq \{\ \|\varphi\|^{\mathfrak{M}} \mid \varphi \in \mathcal{S}_k(\Phi, \Sigma)\ \}$$

is the finite Boolean algebra of denotations of *modal* sentences of modal degree $\leq k$. The modal degree measures depth of nesting of modal operators; for example, for hybrid trajectory formulas of the form (3), the degree is $2n + 1$, where n is the length of the discrete trace. It follows that $\mathcal{S}_{k+1}^{\mathfrak{M}}$ is the smallest Boolean algebra generated by $\mathcal{S}_k^{\mathfrak{M}} \cup \{\sigma(a^{\mathfrak{M}})(A) \mid A \in \mathcal{S}_k^{\mathfrak{M}}\}$. The algorithm terminates at stage $k+1$ if $\mathcal{S}_{k+1}^{\mathfrak{M}} = \mathcal{S}_k^{\mathfrak{M}}$, in which case the equivalence relation:

$$x \approx_{\mathcal{S}_k^{\mathfrak{M}}} y \quad \triangleq \quad (\forall A \in \mathcal{S}_k^{\mathfrak{M}})[\ x \in A \ \Leftrightarrow \ y \in A\ ]$$

is a finite bisimulation equivalence whose equivalence classes are atoms of the algebra $\mathcal{S}_k^{\mathfrak{M}}$, and $\mathcal{S}_\mu^{\mathfrak{M}} = \mathcal{S}_k^{\mathfrak{M}}$.

4 Adding topological and metric tolerance structure

Within modal logic, there is a well-known way of representing a *topology* $\mathcal{T}$ on the state space X of an LTS or Kripke model. From McKinsey and Tarski's work in the 1940's ([31], [32], [36]), the axioms for the box $\Box$ modality of the modal logic **S4** correspond exactly to those of the Kuratowski axioms for the topological interior operator $int_{\mathcal{T}}$, and dually, the **S4** diamond $\Diamond$ corresponds to topological closure $cl_{\mathcal{T}}$. **S4** is a well-studied modal logic, and is of particular interest in virtue of the 1933 Gödel translation of *Intuitionistic* logic into (classical) **S4**. The relational Kripke semantics for **S4** is in terms of *pre-orders*:

[3] The concept is not formally defined here. An analysis of the concept of bisimulation is given in [11]. See also the handbook article [38] §5.3, where it is noted that if one wants to preserve the truth of sentences containing the converse operation, then the notion of bisimulation must be strengthened so as to include respect for the converses of the $a^{\mathfrak{M}}$.

reflexive and transitive relations $\preccurlyeq \subseteq X \times X$, and can be shown to be a special case of the topological semantics via *Alexandroff topologies*, which are in one-one correspondence with pre-orders (see [11]). For background on general topology, see [33], [24].

Let $\mathcal{F}_{\mu,\Box}(\Phi, \Sigma)$ denote the collection of formulas defined as in Definition 3 with an additional clause for a plain $\Box$ modality, with analogous notation for the collection of sentences, and the purely modal fragments. The diamond is defined by the usual negation (de Morgan) duality: $\Diamond\varphi \triangleq \neg\Box\neg\varphi$.

Definition 7. *If $\mathfrak{M} = (X, \mathcal{T}, \{a^{\mathfrak{M}}\}_{a\in\Sigma}, \{\|p\|^{\mathfrak{M}}\}_{p\in\Phi})$ is a* topologized *LTS model then the additional clauses to be added to Definition 4 for the semantics of formulas $\varphi \in \mathcal{F}_{\mu,\Box}(\Phi, \Sigma)$ are:*

$$\|\Box\varphi\|^{\mathfrak{M}}_{\xi} \triangleq int_{\mathcal{T}}\left(\|\varphi\|^{\mathfrak{M}}_{\xi}\right) \quad \textit{and} \quad \|\Diamond\varphi\|^{\mathfrak{M}}_{\xi} \triangleq cl_{\mathcal{T}}\left(\|\varphi\|^{\mathfrak{M}}_{\xi}\right)$$

In the enriched language, we can simply express topological properties of *sets* of states. For example, a set $\|\varphi\|^{\mathfrak{M}} \subseteq X$ is, respectively, *open*, *closed*, *dense* or *nowhere dense* (empty interior), with respect to $\mathcal{T}$, exactly when the sentences $\varphi \to \Box\varphi$, $\Diamond\varphi \to \varphi$, $\Diamond\varphi$, or $\Diamond\neg\varphi$ are true in $\mathfrak{M}$. The topological boundary of $\|\varphi\|^{\mathfrak{M}}$ is denoted by the sentence $\Diamond\varphi \wedge \neg\Box\varphi$ (and boundary sets are always nowhere dense).

Note that if $X \subseteq \mathbb{R}^n$ is first-order definable in an o-minimal structure $\overline{\mathbb{R}}$, $\mathcal{T}$ is the subspace topology on X inherited from the standard metric topology on $\mathbb{R}^n$ (derived from the order $<$ on $\mathbb{R}$), and $A \subseteq X$ is definable, then $int_{\mathcal{T}}(A)$ and $cl_{\mathcal{T}}(A)$ are also definable ([14], Lemma 3.4). Thus if the components of a topologized model $\mathfrak{M}$ are definable in $\overline{\mathbb{R}}$, then the *topological modal algebra*

$$\mathcal{S}^{\mathfrak{M}}_{\Box} \triangleq \{\|\varphi\|^{\mathfrak{M}} \mid \varphi \in \mathcal{S}_{\Box}(\Phi, \Sigma)\}$$

of denotations of modal sentences including $\Box$ is also definable. From the perspective of o-minimality, observe that the cells of a *cell decomposition* of a definable $X \subseteq \mathbb{R}^n$ are either open in $\mathbb{R}^n$, or else are boundary sets ([14], Proposition 2.5) – properties expressible in the enriched modal language.

Note that if we want a bisimulation to be truth-preserving with respect to sentences $\varphi \in \mathcal{S}_{\mu,\Box}(\Phi, \Sigma)$, then it must also respect the topology $\mathcal{T}$. For equivalence relations $\approx$, this amounts to the requirement that for each equivalence class B under $\approx$, the closure $cl_{\mathcal{T}}(B)$ must be a union of equivalence classes, thus either $int_{\mathcal{T}}(B) = B$ or $int_{\mathcal{T}}(B) = \varnothing$; in brief, the equivalence classes B are "cell-like".

OK, so we've formally got topologies in the picture, so we should be able to express *some* notion of *continuity*. A sticking point is that the standard notion of continuity is for *functions*, not relations. In purely topological terms, a *function* $f : (X, \mathcal{T}) \to (Y, \mathcal{S})$ is *continuous* iff for every open set U in Y, the inverse-image $f^{-1}(U)$ is open in X. The relevant notions for relations $r : (X, \mathcal{T}) \rightsquigarrow (Y, \mathcal{S})$ were introduced by Kuratowski and Bouligand in the 1930's, and replace the functional inverse-image with the relational $\forall$- and $\exists$-pre-image operators.

Definition 8. ([6] §1.4; [1][4] Ch. 7; [24] §18.) *A relation* $r : (X, \mathcal{T}) \rightsquigarrow (Y, \mathcal{S})$ *is:*

- upper semi-continuous *(u.s.c.) iff for every open set* U *in* Y*, the* $\forall$*-pre-image* $\tau(r)(U)$ *is open in* X*;*
- lower semi-continuous *(l.s.c.) iff for every open set* U *in* Y*, the* $\exists$*-pre-image* $\sigma(r)(U)$ *is open in* X*;*
- continuous *iff it is both u.s.c. and l.s.c..*

When $r : (X, \mathcal{T}) \rightsquigarrow (Y, \mathcal{S})$ is in fact a (single-valued) function, each of the semi-continuity properties is equivalent to functional continuity, since in that case, the two relational pre-image operators collapse to the familiar inverse-image operator: $\sigma(r) = \tau(r) = r^{-1}$. Logics of continuous functions are developed in [10].

The two semi-continuity properties are simply expressible in the language of the topological μ-calculus by the formulas (sentence schemes):

$$[a]\Box Z \to \Box[a]Z \quad \text{and} \quad \langle a\rangle\Box Z \to \Box\langle a\rangle Z \tag{20}$$

In dual form, upper semi-continuity can be read as preservation of *closed* sets by the familiar $\exists$-pre-image $\sigma(r) = \mathbf{Pre}(r)$:

$$\Diamond\langle a\rangle Z \to \langle a\rangle\Diamond Z$$

From these simple characterizations of the semi-continuity properties, it follows purely formally that each of the properties is inherited under finite relational compositions and finite relational unions (sums). Inheritance of continuity properties under infinitary fixed-point quantification is a topic of continuing investigation.

So far, the discussion of continuity is still rather formal, and a tad insubstantial. But in the case of *compact metric spaces*, we get to see some meat on the bones.

Proposition 1. ([1] Ch.7, Proposition 11) *For relations* $r : X \rightsquigarrow Y$ *where* X *and* Y *are* compact metric spaces *and the direct image* $r(x) \subseteq Y$ *for each* $x \in X$ *is closed, the following are equivalent:*

1. r *is u.s.c.;*
2. *for all* $x \in X$ *and all* $\epsilon > 0$*, there is a* $\delta > 0$ *such that for all* $x' \in X$ *and* $y' \in Y$*,*

$$d_X(x, x') < \delta \;\text{ and }\; x' \xrightarrow{r} y' \;\Rightarrow\; (\exists y \in Y)[\, x \xrightarrow{r} y \;\text{ and }\; d_Y(y, y') < \epsilon\,]$$

3. *as a subset of* $X \times Y$*, (the graph of)* r *is closed;*

[4] Note that in [6], [7], Aubin uses the terms "core" and "inverse-image" instead of universal and existential pre-image, while in [1], Akin uses but has neither names nor notation for the pre-image operators.

4. $\breve{r}: Y \rightsquigarrow X$ *is u.s.c.*

The following are also equivalent:

1. r *is l.s.c.;*
2. *for all* $x \in X$ *and all* $\epsilon > 0$, *there is a* $\delta > 0$ *such that for all* $x' \in X$ *and* $y \in Y$,

$$d_X(x,x') < \delta \;\; \textit{and} \;\; x \xrightarrow{r} y \;\; \Rightarrow \;\; (\exists y' \in Y)[\, x' \xrightarrow{r} y' \;\; \textit{and} \;\; d_Y(y,y') < \epsilon \,]$$

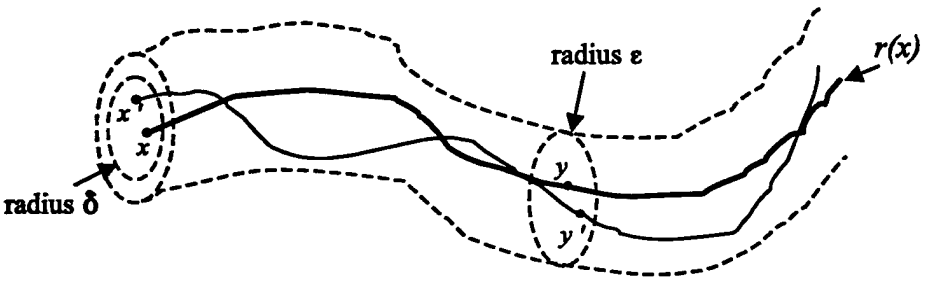

Fig. 4. The u.s.c. property in the compact metric setting.

The metric u.s.c. property says that if an *input* x' is within δ of x, then every point y' in the *output* or image $r(x')$ is contained within an ϵ "ball" or "tube" around $r(x)$. For the orbit relation $f : X \rightsquigarrow X$ of a semi-flow $\phi : X \times \mathbb{R}^+ \to X$ (defined in (11)), where $f(x) = \{\phi(x,t) \mid t \in \mathbb{R}^+\}$ is the positive trajectory from x, the picture really is that of an ϵ-*tube*: if $d_X(x,x') < \delta$ then the trajectory $f(x')$ lies inside an ϵ-tube around the trajectory $f(x)$, as illustrated in Figure 4. The idea is certainly reminiscent of the "tube neighborhoods" in the work of Gupta, Henzinger and Jagadeesan [17] on *robust timed automata*; the interest in that paper is on metrics on trajectories $\tau \in (\Phi \times \mathbb{R}^{>0})^*$, where Φ is a finite alphabet of event names.

When X is a compact metric space, $\phi : X \times \mathbb{R}^+ \to X$ is a continuous semi-flow, and $T \subseteq \mathbb{R}^+$ is compact, the restricted orbit relation $f^T : X \rightsquigarrow X$ given by $f^T(x) = \{\phi(x,t) \mid t \in T\}$ has a closed graph and hence is u.s.c. ([1], Ch. 6). This leads to the following result on continuity properties of *both* sort of transition relations in an LTS model of a hybrid automaton.

Proposition 2. *Let* $\mathfrak{M}_{\mathcal{H}}$ *be the LTS model of a hybrid automaton, as in Definition 2. Assume that each* $X_q \subseteq \mathbb{R}^n$ *is compact in the standard topology on* $\mathbb{R}^n$. *Let* $\mathcal{T}_q$ *be the subspace topology on* X_q, *and assume the semi-flow* $\phi_q : X_q \times \mathbb{R}^+ \to X_q$ *is continuous.*

1. *If* Inv_q *is* closed *in* $\mathcal{T}_q$, *and* time-bounded *under* ϕ_q, *in the sense that there is a* $t_q > 0$ *such that for all* $x \in Inv_q$ *and all* $t > t_q$, $\phi_q(x,t) \notin Inv_q$, *then the relation* $e_q : X_q \rightsquigarrow X_q$ *defined by* $e_q = f_q \cap (Inv_q \times Inv_q)$ *is u.s.c..*

2. *If* $Grd_{q,q'} \subseteq X_q$ *and* $Inv_{q'} \subseteq X_{q'}$ *are both closed, in* $\mathcal{T}_q$ *and* $\mathcal{T}_{q'}$ *respectively, and the graph of* $r_{q,q'} : X_q \rightsquigarrow X_{q'}$ *is closed,*
then the relation $c_{q,q'} : X_q \rightsquigarrow X_{q'}$ *defined by* $c_{q,q'} = r_{q,q'} \cap (Grd_{q,q'} \times Inv_{q'})$ *is u.s.c..*

The point is that the u.s.c. property is sufficiently attractive that we may wish it to be the case that *all* our transition relations possess it. From our observations above, all finite compositions and unions of the e_q and $c_{q,q'}$ will be u.s.c. if the e_q and $c_{q,q'}$ are u.s.c.. Note also that for the *constant* jump relations $c_{q,q'} = Grd_{q,q'} \times Rst_{q,q'}$ of [27], $c_{q,q'}$ is u.s.c. when both $Grd_{q,q'}$ and $Rst_{q,q'}$ are closed.

When the relations $e_q : X_q \rightsquigarrow X_q$ and $c_{q,q'} : X_q \rightsquigarrow X_{q'}$ are lifted to relations $X \rightsquigarrow X$, the issue arises as to what is the appropriate topology on the *hybrid state space* $X \subseteq Q \times \mathbb{R}^n$? Taking the X_q equipped with their standard topology from $\mathbb{R}^n$, the question then becomes: what topology $\mathcal{T}_Q$ on the finite discrete state space Q? One reasonable choice is that Q really is *discrete* and has no topological structure, which amounts to taking $\mathcal{T}_Q$ to be the discrete topology. Then the lifted relations will be u.s.c. or l.s.c. whenever their unlifted counterparts are. An alternative reasonable choice is to consider Q as structured by the control graph $G \subseteq Q \times Q$, so take $\mathcal{T}_Q = \mathcal{T}_G$ to be the (Alexandroff) topology determined by the reflexive-transitive closure $\preccurlyeq_G$ of G. The open (closed) sets in $\mathcal{T}_G$ are those $P \subseteq Q$ that are up- (down-) *invariant* under $\preccurlyeq_G$; the clopen sets in $\mathcal{T}_G$ are *cycles* under G. The inherited topology on $X \subseteq Q \times \mathbb{R}^n$, and the continuity properties, are more complicated, and under current investigation.

Metric structure on the state space of an LTS model can be used to define explicit *metric tolerance relations* that allow us to express such properties as *being within* ϵ *of a set*, for a particular $\epsilon > 0$. Again, the resources of modal logic come into play. For X a metric space and $\epsilon > 0$, define a relation of ϵ-*tolerance* or ϵ-*indiscernability* $(\epsilon) : X \rightsquigarrow X$ by:

$$x \ (\epsilon) \ x' \quad \text{iff} \quad d_X(x, x') < \epsilon \tag{21}$$

Such a relation is *reflexive* and *symmetric*, but not transitive. My source for the notion of a tolerance relation is Smyth's [37]. A motivating idea in that paper, which is traced back to Poincaré's *The Value of Science*1905) and independently, to the topologist Zeeman in the early 1960's, is that *perceptual* or *physical* continua, as opposed to the *idealized* continua of classical mathematics, are of finite or countable cardinality and are structured by a relation of indiscernability that is reflexive and symmetric, but not transitive. In [1] Ch.1, the relation (ϵ) goes by the name V_ϵ.

Formally, we extend the alphabet Σ of transition labels with a new symbol ϵ. Interpreting the new modalities $\langle\epsilon\rangle$ and $[\epsilon]$ in the standard way by the pre-image operators $\sigma(\epsilon)$ and $\tau(\epsilon)$, the sentence $\langle\epsilon\rangle\varphi$ denotes the ϵ-*ball* around $\|\varphi\|^{\mathfrak{M}}$, or the ϵ-*closure* of $\|\varphi\|^{\mathfrak{M}}$ – that is, the set of states within ϵ of *some* point in $\|\varphi\|^{\mathfrak{M}}$, while $[\epsilon]\varphi$ denotes the ϵ-*interior* of $\|\varphi\|^{\mathfrak{M}}$ – that is, the set of states *all* of whose

ϵ-neighbors are in $\|\varphi\|^{\mathfrak{M}}$. The modalities for symmetric and reflexive relations are axiomatized by the modal logic **KTB**; see [9] §4.3.

The combination of topological and tolerance structure opens up new possibilities. For example ([1] Ch.1, Corollary 2), if $a^{\mathfrak{M}} : X \rightsquigarrow X$ is u.s.c. in a compact metric space X, then for each *closed* set $\|\varphi\|^{\mathfrak{M}} \subseteq X$, and each $\epsilon > 0$, there is a $\delta > 0$ such that the sentence

$$\langle\delta\rangle\langle a\rangle\varphi \to \langle a\rangle\langle\epsilon\rangle\varphi \tag{22}$$

is true in $\mathfrak{M}$.

Metric tolerance structure can be used to define "imperfect precision" hybrid trajectories. In the LTS model $\mathfrak{M}_{\mathcal{H}}$ of a hybrid automaton $\mathcal{H}$, suppose that on each projection $X_q \subseteq \mathbb{R}^n$, we have a metric tolerance $(\delta_q) : X_q \rightsquigarrow X_q$ for some given $\delta_q > 0$. Then instead of considering "perfect precision" trajectories formed from the simple alternation of constrained evolution and controlled jump relations, as in (3), we might want to consider transition sequences:

$$e_{q_0} \cdot \delta_{q_0} \cdot c_{q_0,q_1} \cdot e_{q_1} \cdot \delta_{q_1} \cdot c_{q_1,q_2} \cdot e_{q_2} \cdot \cdots \cdot e_{q_{k-1}} \cdot \delta_{q_{k-1}} \cdot c_{q_{k-1},q_k} \cdot e_{q_k} \tag{23}$$

Operationally, this can be construed as allowing metric "gaps" of up to size δ_q between the *decision* to make a controlled switch $c_{q,q'}$, and the point at which such a *switch actually occurs*. Defining $(\delta) : X \rightsquigarrow X$ to be the union of each of the lifted relations (δ_q), the dynamics of the class of all "δ-imperfect" hybrid trajectories with finite discrete traces are captured by the dual fixed-point modalities

$$\langle\mathbf{h}_\delta\rangle\varphi \triangleq \mu Z.\, \langle\mathbf{e}\rangle\varphi \vee \langle\mathbf{e}\rangle\langle\delta\rangle\langle\mathbf{c}\rangle Z \quad \text{and} \quad [\mathbf{h}_\delta]\varphi \triangleq \nu Z.\, [\mathbf{e}]\varphi \wedge [\mathbf{e}][\delta][\mathbf{c}] Z \tag{24}$$

Alternatively, one could "relax" the definition of the constrained evolution relation, and take

$$\langle\dot{\mathbf{e}}_q\rangle Z \leftrightarrow \langle\delta_q\rangle\mathbf{Inv}_q \wedge \langle\mathbf{f}_q\rangle(Z \wedge \mathbf{Inv}_q)$$

that is, $\dot{e}_q = f_q \cap (Inv_q \times \sigma(\delta_q) Inv_q)$, where the revised convexity property is:

$$\langle\breve{\mathbf{f}}_q\rangle\mathbf{Inv}_q \wedge \langle\mathbf{f}_q\rangle\langle\delta_q\rangle\mathbf{Inv}_q \to \langle\delta_q\rangle\mathbf{Inv}_q$$

which says: curves along ϕ_q that start in Inv_q and end in $\sigma(\delta_q) Inv_q$ lie inside $\sigma(\delta_q) Inv_q$.

5 Deductive Proof Systems

We present simple Hilbert-style axiomatic proof systems for the logics of interest. The axiomatizations are not intended to be minimal; rather, they are meant to

serve as a useful reference list. In particular, we give the axioms and rules for both of the dual diamond and box modalities. Kozen's axiomatization $\mathbf{L}_\mu$ [23] forms the foundation, with extensions developed in a modular fashion. So far, we have identified **S4** for topological and relational pre-order modalities, and **KTB** for tolerance relations. A further candidate is **S5**, the modal logic of *equivalence relations*: we can give modal representation to any partition of the state space of our choosing; bisimulation equivalences spring to mind. **S5** is also the base of *logics of knowledge* [16]: the knowledge of an agent is modeled by the equivalence relation of indistinguishability relative to its knowledge base.

Equivalent Gentzen sequent-style proof systems for the μ-calculus are presented in [5], [8], and also in [40].

Definition 9. *The Hilbert-style proof system for the logic* $\mathbf{L}_\mu$ *has the following axioms: for transition labels* $a \in \Sigma$*, propositional variables* $Z, W \in \mathrm{PVar}$*, and formulas* $\varphi \in \mathcal{F}_\mu(\Phi, \Sigma)$*,*

CP :	*axioms of classical propositional logic*		
$\vee$-$\langle a\rangle$:	$\langle a\rangle(Z \vee W) \leftrightarrow (\langle a\rangle Z \vee \langle a\rangle W)$	**ff**-$\langle a\rangle$:	$\langle a\rangle\mathbf{ff} \leftrightarrow \mathbf{ff}$
$\wedge$-$[a]$:	$[a](Z \wedge W) \leftrightarrow ([a]Z \wedge [a]W)$	**tt**-$[a]$:	$[a]\mathbf{tt} \leftrightarrow \mathbf{tt}$
μ-*f.p.* :	$\varphi[Z := \mu Z.\varphi] \rightarrow \mu Z.\varphi$	ν-*f.p.* :	$\nu Z.\varphi \rightarrow \varphi[Z := \nu Z.\varphi]$

and the inference rules, for formulas $\varphi, \psi \in \mathcal{F}_\mu(\Phi, \Sigma)$*:*

$$\textit{modus ponens:} \quad \frac{\varphi,\ \varphi \rightarrow \psi}{\psi}$$

$$\textit{substitution:} \quad \frac{\varphi}{\varphi[Z := \psi]}$$

$$\langle a\rangle\textit{-monotonicity:} \quad \frac{\varphi \rightarrow \psi}{\langle a\rangle\varphi \rightarrow \langle a\rangle\psi}$$

$$[a]\textit{-monotonicity:} \quad \frac{\varphi \rightarrow \psi}{[a]\varphi \rightarrow [a]\psi}$$

$$\mu\textit{-least-f.p.:} \quad \frac{\varphi[Z := \psi] \rightarrow \psi}{\mu Z.\varphi \rightarrow \psi}$$

$$\nu\textit{-greatest-f.p.:} \quad \frac{\psi \rightarrow \varphi[Z := \psi]}{\psi \rightarrow \nu Z.\varphi}$$

$$\textit{Hoare composition:} \quad \frac{\psi \rightarrow \langle a\rangle\chi \quad \chi \rightarrow \langle b\rangle\varphi}{\psi \rightarrow \langle a\rangle\langle b\rangle\varphi}$$

$$\textit{Hoare composition:} \quad \frac{\psi \rightarrow [a]\chi \quad \chi \rightarrow [b]\varphi}{\psi \rightarrow [a][b]\varphi}$$

We write: $\mathbf{L}_\mu \vdash \varphi$ for formulas $\varphi \in \mathcal{F}_\mu(\Phi, \Sigma)$ if there is a proof of φ in $\mathbf{L}_\mu$.

The axioms and monotonicity rules for $\langle a \rangle$ and $[a]$ together assert they are *normal* diamond (possibility) and box (necessity) modalities ([9] Ch. 4); they are equivalent to system **K** (for Kripke), the logic of generic binary relations. In the language of [26], $\langle a \rangle$ denotes a *normal and finitely additive* operator on a Boolean algebra. The Hoare composition rules follow readily from monotonicity. As always, we assume substitutions $\varphi[Z := \psi]$ are legitimate ones; i.e. no capture of free variables.

The axioms and rules for the fixed-point quantifiers assert what they ought: that $\mu Z.\varphi$ ($\nu Z.\varphi$) is the least (greatest) fixed point of the operator defined by φ.

Each of the rules is readily verified to be *truth-preserving*, in the sense that for any LTS model $\mathfrak{M}$, if the hypotheses of a rule is true in $\mathfrak{M}$ then the conclusion is true in $\mathfrak{M}$. From the verification that the each of the axioms is true in every LTS model, we then get *soundness*: if $\boldsymbol{L}_\mu \vdash \varphi$ then $\mathfrak{M} \models \varphi$ for all LTS models $\mathfrak{M}$ of signature (Φ, Σ).

Definition 10. *The Hilbert-style proof system for the logic* $\mathbf{L}_\mu + \mathbf{S4}$ *in the language* $\mathcal{F}_{\mu,\Box}(\Phi, \Sigma)$ *is obtained from that of* $\mathbf{L}_\mu$ *by adding the normality axioms and rules for* $\Diamond$ *and* $\Box$*, together with: for propositional variables* $Z \in \mathrm{PVar}$*,*

$$\mathbf{T}\Diamond: \ Z \to \Diamond Z \qquad \mathbf{T}\Box: \ \Box Z \to Z$$
$$\mathbf{4}\Diamond: \ \Diamond\Diamond Z \to \Diamond Z \qquad \mathbf{4}\Box: \ \Box Z \to \Box\Box Z$$

The proof system for the logic $\mathbf{L}_\mu + \mathbf{S4} + C_a$ *is that of* $\mathbf{L}_\mu + \mathbf{S4}$ *together with* C_a*, where* C_a *is one or more of the semi-continuity axiom schemes:*

$$\mathbf{usc}\langle a \rangle: \ \Diamond\langle a \rangle Z \to \langle a \rangle \Diamond Z \qquad \mathbf{usc}[a]: \ [a]\Box Z \to \Box[a] Z$$
$$\mathbf{lsc}\langle a \rangle: \ \langle a \rangle \Box Z \to \Box\langle a \rangle Z \qquad \mathbf{lsc}[a]: \ \Diamond[a] Z \to [a]\Diamond Z$$

In the relational (preorder) semantics for **S4**, the **T** axioms correspond to reflexivity, while the **4** axioms correspond to transitivity. Extensions of the Hoare composition rules:

$$\frac{\psi \to [a]\Box\chi \quad \chi \to [b]\Box\varphi}{\psi \to [a][b]\Box\varphi} \quad \text{and} \quad \frac{\psi \to \langle a \rangle\Box\chi \quad \chi \to \langle b \rangle\Box\varphi}{\psi \to \langle a \rangle\langle b \rangle\Box\varphi}$$

can be derived in the systems $\boldsymbol{L}_\mu + \mathbf{S4} + \boldsymbol{usc}[a] + \boldsymbol{usc}[b]$ and $\boldsymbol{L}_\mu + \mathbf{S4} + \boldsymbol{lsc}\langle a \rangle + \boldsymbol{lsc}\langle b \rangle$ respectively.

Definition 11. *The Hilbert-style proof system for the logic* $\mathbf{L}_\mu + \mathbf{KTB}$ *in the language* $\mathcal{F}_\mu(\Phi, \Sigma \cup \{\epsilon\})$ *is obtained from that of* $\mathbf{L}_\mu$ *by adding the normality axioms and rules for* $\langle \epsilon \rangle$ *and* $[\epsilon]$*; the axioms* $\mathbf{T}\langle \epsilon \rangle$ *and* $\mathbf{T}[\epsilon]$*; and also:*

$$\mathbf{B}\langle \epsilon \rangle: \ \langle \epsilon \rangle [\epsilon] Z \to Z \qquad \mathbf{B}[\epsilon]: \ Z \to [\epsilon]\langle \epsilon \rangle Z$$

The **B** axioms express that tolerance relations (ϵ) are symmetric.

Definition 12. *The Hilbert-style proof system for the logic* $\mathbf{L}_\mu + \mathbf{S5}$ *in the language* $\mathcal{F}_\mu(\Phi, \Sigma \cup \{\approx\})$ *is obtained from that of* $\mathbf{L}_\mu$ *by adding the normality axioms and rules for* $\langle\approx\rangle$ *and* $[\approx]$*; the axioms* $\mathbf{T}\langle\approx\rangle$, $\mathbf{T}[\approx]$, $\mathbf{4}\langle\approx\rangle$ *and* $\mathbf{4}[\approx]$*; and also:*

$$\mathbf{5}\langle\approx\rangle: \ \langle\approx\rangle[\approx]Z \to [\approx]Z \qquad \mathbf{5}[\approx]: \ \langle\approx\rangle Z \to [\approx]\langle\approx\rangle Z$$

The **5** axioms express that $\approx$ is a *Euclidean* relation: if $x \approx y$ and $x \approx z$ then $y \approx z$. And reflexive, transitive and Euclidean binary relations are exactly equivalence relations. Under the knowledge interpretation of **S5**, the axiom $\mathbf{5}[\approx]$ is usually referred to as the axiom of *negative introspection*: $\neg[\approx]\varphi \to [\approx]\neg[\approx]\varphi$, which reads: "if it is not the case that agent A knows φ, then agent A knows that it is not the case that she knows φ".

Walukiewicz has recently established the completeness of the Kozen axiomatization with respect to the standard set-theoretic semantics for the μ-calculus.

Theorem 1. ([39],[40]) Soundness and Completeness of $\mathbf{L}_\mu$ (set-theoretic semantics)
For all formulas $\varphi \in \mathcal{F}_\mu(\Phi, \Sigma)$,
$\mathbf{L}_\mu \vdash \varphi$ *iff* $\mathfrak{M} \models \varphi$ *for all LTS models* $\mathfrak{M}$ *of signature* (Φ, Σ).

The completeness part of the cited theorem is stated in the form: if φ is *unsatisfiable* in every LTS model $\mathfrak{M}$, i.e. $\|\varphi\|^{\mathfrak{M}}_\xi = \emptyset$ for all assignments ξ in $\mathcal{P}(X)$, then $\neg\varphi$ is provable in $\mathbf{L}_\mu$.Walukiewicz's proof is very intricate, proceeding by first contracting to a subclass of "nice" formulas, and then producing a "tableaux refutation" of unsatisfiable formulas of nice form, where such a refutation in turn implies that the negation of the given formula is provable in $\mathbf{L}_\mu$. Topics of continuing enquiry include whether the Walukiewicz proof can be extended to cover specific modal enrichments of $\mathbf{L}_\mu$, and the relationship between his tableaux refutation system and a tableaux proof system for the μ-calculus and polymodal extensions, in the style of [35] and [10].

The algebraic semantics of Kwiatkowska *et al.* [5], [8], provide a framework for extending Stone duality theory to the algebra of fixed-points. Their proof of completeness for modal μ-frames starts with the Lindenbaum algebra $\mathcal{F}_{\mathbf{L}_\mu}$ of formulas in $\mathcal{F}_\mu(\Phi, \Sigma)$ modulo provable equivalence in $\mathbf{L}_\mu$, then realizes the abstract μ-algebra as a canonical LTS model $\mathfrak{M}_{\mathbf{L}_\mu}$ with state space the Stone space $X = Ult(\mathcal{F}_{\mathbf{L}_\mu})$ of (Boolean) ultrafilters in $\mathcal{F}_{\mathbf{L}_\mu}$, together with the canonical μ-algebra $\mathcal{A}_{\mathbf{L}_\mu} = Clop(Ult(\mathcal{F}_{\mathbf{L}_\mu})) \cong \mathcal{F}_{\mathbf{L}_\mu}$ of subsets of X clopen in the Stone topology. For each $a \in \Sigma$, and $\mathfrak{M} = \mathfrak{M}_{\mathbf{L}_\mu}$, the relations $a^{\mathfrak{M}}$ on X are defined by: $x \xrightarrow{a^{\mathfrak{M}}} y$ iff $(\forall \overline{\varphi} \in \mathcal{F}_{\mathbf{L}_\mu})[\, \overline{[a]\varphi} \in x \ \Rightarrow \overline{\varphi} \in y \,]$. The formal statement of the result is as follows.

Theorem 2. ([5]) Soundness and Completeness of $\mathbf{L}_\mu$ (algebraic semantics)
For all formulas $\varphi \in \mathcal{F}_\mu(\Phi, \Sigma)$,
$\mathbf{L}_\mu \vdash \varphi$ *iff* $(\mathfrak{M}, \mathcal{A}) \models \varphi$ *for all modal* μ*-frames* $(\mathfrak{M}, \mathcal{A})$ *of signature* (Φ, Σ).

In [8] §6, it is established if $(\mathfrak{M}, \mathcal{A})$ is a *descriptive* modal μ-frame, then $(\mathfrak{M}, \mathcal{A})$ is in semantic agreement with $\mathfrak{M}$. In particular, the canonical frame $(\mathfrak{M}_{\mathbf{L}_\mu}, \mathcal{A}_{\mathbf{L}_\mu})$ is descriptive, and thus in semantic agreement with the underlying LTS model $\mathfrak{M}_{\mathbf{L}_\mu}$. Thus the "easy" algebraic proof of completeness can be used to give an alternative proof of completeness of $\mathbf{L}_\mu$ with respect to the standard set-theoretic semantics, as stated in Theorem 1.

The Kwiatkowska algebraic completeness proof extends quite smoothly to normal polymodal extensions of the μ-calculus, including topological **S4** extensions with semi-continuity axioms. For example, if $\mathbf{L} = \mathbf{L}_\mu + \mathbf{S4} + \{\mathbf{usc}[a] + \mathbf{lsc}\langle a\rangle\}_{a\in\Sigma}$, the topology on the canonical model $\mathfrak{M}_\mathbf{L}$ comes from a relation $\preccurlyeq$ on $X = Ult(\mathcal{F}_\mathbf{L})$ defined in the same way as the relations $a^{\mathfrak{M}_\mathbf{L}}$ as above. The **S4** axioms ensure that the relation $\preccurlyeq$ is a preorder, so the topology is Alexandroff, and from the semi-continuity axiom schemes, one proves that each of the relations $a^{\mathfrak{M}_\mathbf{L}}$ have the corresponding semi-continuity property. A more detailed treatment is given in [12].

6 Discussion

We have developed a family of expressively rich and usable logical systems and broadened horizons for the formal analysis of hybrid dynamical systems. In addition to those mentioned in the text, further lines of enquiry include the following.

- Investigation of non-deterministic continuous dynamics, in the form of set-valued or parametrized semi-flows, and their topological properties. Our relation-based view of dynamics is of course conducive to such generalizations.
- A deeper investigation of relations (definable families) in o-minimal structures, and of the use of finite cell-decomposition in the construction of *topological* bisimulations.
- Further investigation of finite sub-topologies of the standard topology on $X \subseteq \mathbb{R}^n$, and semi-continuity properties of relations in such topologies, pursuing themes developed in [11].
- Application to hybrid systems of the theory of knowledge in multi-agent settings and its formalization in **S5** based logics of knowledge.
- LTS models and μ-calculus specifications of *hybrid petri nets*. One approach is to take the state space X to be a set of finite partial functions $x : P \rightsquigarrow \mathbb{R}$ (equivalently, variable-length vectors over $\mathbb{R}$), where P is the finite set of *places* of the net.
- Application of game-theoretic methods for the μ-calculus, and related work on automata over transition systems; e.g. [25], [22].
- Investigation of *tableaux proof systems* for polymodal logics and the μ-calculus, in the style of [35] and [10].
- Investigation of *Intuitionistic* (constructive) logics for hybrid systems, using topological semantics and **S4** as a bridge between the classical and constructive worlds.

Acknowledgments: I would like to thank Prof. Anil Nerode, David Cook, Joe Miller, Suman Ganguli and Prof. Dexter Kozen for valuable conversations, and Xi Krump for graphic artistry.

References

1. E. Akin, *The General Topology of Dynamical Systems*, Graduate Studies in Mathematics 1 (American Mathematical Society, Providence, 1993).
2. R. Alur, C. Courcoubetis, N. Halbwachs, T. A. Henzinger, P.-H. Ho, X. Nicollin, A. Olivero, J. Sifakis and S. Yovine, "The Algorithmic Analysis of Hybrid Systems", *Theoretical Computer Science* **138** (1995) 3-34.
3. R. Alur and D. L. Dill, "A Theory of Timed Automata", *Theoretical Computer Science* **126** (1994) 183-235.
4. R. Alur, T. A. Henzinger and P.-H. Ho, "Automatic Symbolic Verification of Embedded Systems", *IEEE Transactions on Software Engineering* **22** (1996) 181-201.
5. S. Ambler, M. Kwiatkowska and N. Measor, "Duality and the Completeness of the Modal μ-calculus", *Theoretical Computer Science* **151** (1995) 3-27.
6. J-P. Aubin and H. Frankasowa, *Set-Valued Analysis* (Birkhäuser, Boston, 1990).
7. J-P. Aubin, *Viability Theory* (Birkhäuser, Boston, 1991).
8. M. M. Bonsangue and M. Z. Kwiatkowska, "Reinterpreting the Modal μ-calculus", in A. Ponse, M. de Rijke and Y. Venema (eds.), *Modal Logic and Process Algebra*, CSLI Lecture Notes **53** (CLSI Publications, Stanford, 1995); 65-83.
9. B. F. Chellas, *Modal Logic: An Introduction* (Cambridge University Press, 1980).
10. J. M. Davoren, *Modal Logics for Continuous Dynamics*, PhD dissertation, Department of Mathematics, Cornell University, January 1998.
11. J. M. Davoren, "Topologies, Continuity and Bisimulations", presented at Fixed Points in Computer Science, Brno, August 1998; submitted for publication.
12. J. M. Davoren, "On Continuous Dynamics and Modal Logics", in preparation.
13. C. Daws, A. Olivero, S. Tripakis and S. Yovine, "The Tool KRONOS", in R. Alur, T. A. Henzinger and E. D. Sontag (eds.), *Hybrid Systems III*, Lecture Notes in Computer Science **1066** (Springer-Verlag, Berlin, 1996); 208-219.
14. L. van den Dries, *Tame Topology and O-minimal Structures*, London Mathematical Society Lecture Notes Series **248** (Cambridge University Press, 1998).
15. E. A. Emerson, "Modal Checking and the Mu-calculus", in N. Immerman and P. G. Kolaitis (eds.), *Descriptive Complexity and Finite Models*, DIMACS Series in Discrete Mathematics and Theoretical Computer Science **31** (American Mathematical Society, Providence, 1997); 185-208.
16. R. Fagin, J. Y. Halpern, Y. Moses and M. Y. Vardi, *Reasoning About Knowledge* (MIT Press, Cambridge MA, 1995).
17. V. Gupta, T. A. Henzinger and R. Jagadeesan, "Robust Timed Automata", in O. Maler (ed.), *Hybrid and Real-Time Systems: International Workshop HART'97, March 1997*, Lecture Notes in Computer Science **1201** (Springer-Verlag, Berlin, 1997); 331-345.
18. L. Henkin, "Completeness in the Theory of Types", *Journal of Symbolic Logic* **15** (1950) 81-91.
19. T. A. Henzinger, "The Theory of Hybrid Automata", *Proceedings of the 11$^{\text{th}}$ Annual IEEE Symposium on Logic in Computer Science (LICS '96)* (IEEE Computer Society Press, 1996); 278-292.

20. T. A. Henzinger, O. Kupferman, and S. Qadeer, "From *Pre*-historic to *Post*-modern Symbolic Model Checking", *Proceedings of the Tenth International Conference on Computer-aided Verification (CAV 1998)*, Lecture Notes in Computer Science (Springer-Verlag, Berlin, 1998).
21. T. A. Henzinger, Z. Manna and A. Pnueli, "Towards Refining Temporal Specifications into Hybrid Systems", in R. Grossman *et al.* (eds.), *Hybrid Systems*, Lecture Notes in Computer Science **736** (Springer-Verlag, Berlin,1993), 60-76.
22. M. J. Hollenberg, *Logic and Bisimulation*, PhD dissertation, Department of Philosophy, Utrecht University, March 1998.
23. D. Kozen, "Results on the Propositional μ-Calculus", *Theoretical Computer Science* **27** (1983) 333-354.
24. K. Kuratowski, *Topology, Volume 1*, revised edition (Academic Press, New York, 1966). Translated by J. Jaworowski from the French 1958 edition of *Topologie, Volume 1*, Polska Akademia Nauk Monografie Matematyczne, Tom **21** (Państwowe Wydawnictwo Naukowe, Warsaw, 1958).
25. D. Janin and I. Walukiewicz, "On the expressive completeness of the propositional mu-calculus with respect to monadic second order logic", *Proceedings of the Seventh International Conference on Concurrency Theory (CONCUR'96)*, Lecture Notes in Computer Science **1119** (Springer-Verlag, Berlin, 1996), 263–277.
26. B. Jónsson and A. Tarski, "Boolean Algebras with Operators, Part I", *American Journal of Mathematics* 73 (1951) 891–939.
27. G. Lafferriere, G. J. Pappas and S. Sastry, "O-Minimal Hybrid Systems", Technical report UCB/ERL M98/29, Department of Electrical Engineering and Computer Science, University of California at Berkeley, May 1998.
28. G. Lafferriere, G. J. Pappas and S. Yovine, "Decidable Hybrid Systems", Technical report UCB/ERL M98/39, Department of Electrical Engineering and Computer Science, University of California at Berkeley, June 1998.
29. Z. Manna and A. Pnueli, "Verifying Hybrid Systems", in R. Grossman *et al.* (eds.), *Hybrid Systems*, Lecture Notes in Computer Science **736** (Springer-Verlag, Berlin,1993), 4-35.
30. Z. Manna and H. B. Simpa, "Deductive Verification of Hybrid Systems Using STeP", in T. A. Henzinger and S. Sastry (eds), *Hybrid Systems-Computation and Control: Proceedings of the First International Workshop (HSCC '98)*, Lecture Notes in Computer Science **1386**, (Springer-Verlag, Berlin, 1998).
31. J. C. C. McKinsey, "A Solution of the Decision Problem for the Lewis Systems S2 and S4, with an Application to Topology", *Journal of Symbolic Logic* **6** (1941) 117-134.
32. J. C. C. McKinsey and A. Tarski, "The Algebra of Topology", *Annals of Mathematics* **45** (1944) 141-191.
33. J. R. Munkres, *Topology: A First Course* (Prentice Hall, Englewood Cliffs, 1975).
34. A. Nerode and W. Kohn, "Models for Hybrid Systems: Automata, Topologies, Controllability, Observability", in R. Grossman *et al.* (eds.), *Hybrid Systems*, Lecture Notes in Computer Science **736** (Springer-Verlag, Berlin,1993), 297-316.
35. A. Nerode and R. Shore, *Logic for Applications* (2nd ed.), Graduate Texts in Computer Science (Springer-Verlag, Berlin, 1997).
36. H. Rasiowa and R. Sikorski, *The Mathematics of Metamathematics*, Polska Akademia Nauk Monografie Matematyczne, Tom **41** (Państwowe Wydawnictwo Naukowe, Warsaw, 1963).
37. M. B. Smyth, "Semi-metrics, closure spaces and digital topology", *Theoretical Computer Science* **151** (1995) 257-276.

38. C. Stirling, "Modal and Temporal Logics", in S. Abramsky, D. M. Gabbay and T. Maibaum (eds.), *Handbook of Logic in Computer Science, Vol. 2: Computational Structures* (Oxford University Press, Clarendon Press, Oxford, 1992), 477-563
39. I. Walukiewicz, "On Completeness of the μ-calculus", *Proceedings of the 8th Annual IEEE Symposium on Logic in Computer Science* (LICS '93) (IEEE Computer Society Press, 1993); 136-146.
40. I. Walukiewicz, "A Note on the Completeness of Kozen's Axiomatization of the Propositonal μ-calculus", *Bulletin of Symbolic Logic* **2** (1996) 349-366.